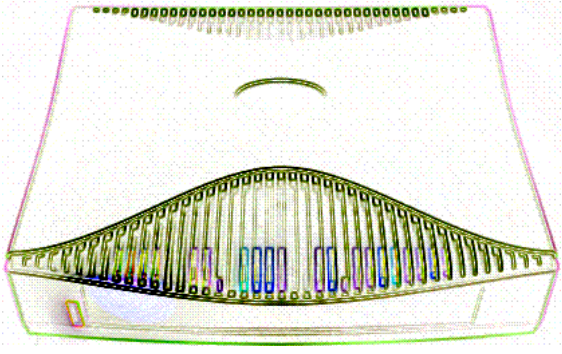
NETOPIA™ R910 ETHERNET ROUTER FOR DSL AND CABLE MODEMS

User's Reference Guide



netopia®

Copyright

Netopia, Inc.
2470 Mariner Square Loop
Alameda, CA 94501-1010
U.S.A.

Part Number

For additional copies of this electronic manual, order Netopia part number 6161087-PF-01

Printed Copies

For printed copies of this manual, order Netopia part number TER910/Doc
(P/N 6161087-00-01)

Contents

Chapter 1

Introduction

Overview

The Netopia R910 Ethernet Router is a stand-alone, multiprotocol broadband router for connecting diverse local area networks (LANs) to the Internet and other remote networks. Combining the Netopia R910 with a cable or DSL modem provides businesses with a low-cost connection to the Internet while retaining the power of a router. Once your Netopia R910 Ethernet Router is connected to your LAN and an Internet connection device such as a cable or a DSL modem, and your account is activated by your network service provider, you will have a high-speed connection between your LAN and the telephone company's network of high-speed digital facilities.

This section covers the following topics:

Features and capabilities

The Netopia R910 Ethernet Router provides the following features:

- Always-on connection eliminates dialing and provides lower, more predictable transmission costs.
- Interconnects with cable modems or DSL modems or bridges that have an Ethernet port.
- Connectivity to support Ethernet LANs via built-in 4-port 10Base-T hub.
- Support for Network Address Translation (NAT) and MultiNAT, allowing all computers and IP hosts on the LAN to appear as one or more IP addresses to the ISP on the WAN link.
- Support for DHCP, allowing automatic assignment of IP addresses on the LAN or WAM and simplyfying configuration and management.
- Support for VPN client and server, supporting remote VPN clients as well as providing a single connection for all or select VPN clients on the LAN. Supports PPTP-based VPN for interoperability with Windows Dial-Up Networking and IPSec for secure public key encryption.
- Status lights (LEDs) for easy monitoring and troubleshooting.
- Support for IP routing for Internet and intranet connectivity.
- Support for console-based management over Telnet or serial cable connection.
- Support for remote configuration by your reseller, your network administrator, or technicians at Netopia, Inc., via IP network.
- Wall-mountable, bookshelf (side-stackable), or desktop-stackable design for effective space usage.

How to use this guide

This guide is designed to be your single source for information about your Netopia R910 Ethernet Router. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

If you prefer to work from hard copy rather than on-line documentation, you can also print out all of the manual, or individual sections. The pages are formatted to print on standard 8 1/2 by 11 inch paper. We recommend that you print on three-hole punched paper, so you can put the pages in a binder for future reference. For your convenience, a printed copy can be purchased from Netopia. Order part number TER910/Doc.

This guide is organized into chapters describing the Netopia R910's advanced features. You may want to read each chapter's introductory section to familiarize yourself with the various features available.

Use the guide's table of contents and index to locate informational topics.

Chapter 2

Setting Up Internet Services

This chapter describes how to obtain and set up Internet services.

This section covers the following topics:

Deciding on an ISP account

Your ISP may offer various Internet access account plans. Typically, these plans vary by usage charges and the number of host IP addresses supplied. Evaluate your networking needs and discuss them with your ISP before deciding on a plan for your network.

DSL and cable modems

Many ISPs offer economical service plans that connect to the DSL or cable network using a DSL or cable modem. Unlike V.90 or V.32 analog modems, which typically were installed directly into your computer or were connected serially, DSL and cable modems typically connect over Ethernet. With Ethernet, your ISP can offer you a service connecting one or more computers. Using NAT and MultiNAT features, you can configure your Netopia router to give all computers, printers, and other IP hosts access to the Internet using one or a limited number of IP addresses. This means that you have more flexibility in selecting ISP account types. The most affordable single IP account may be sufficient for your needs. With the router configured for NAT all users on the LAN have access to the Internet, yet you're using just the one IP address assigned by your ISP.

The Netopia router offers another benefit to DSL and cable modem users. Because a DSL or cable modem connects your computers directly to the Internet with a static IP address, you are more vulnerable to hackers or would-be intruders. The Netopia R910 Ethernet Router is installed between the DSL or cable modem and the computer, printer, and other IP hosts on the LAN, and induces a firewall to deflect hackers and intruders.

Obtaining information from the ISP

After your account is set up, the ISP should send you the IP parameter information that will help you configure the Netopia R910.

Local LAN IP address information to obtain

Your ISP will need to provide you with the following information:

- The default gateway IP address
- Remote IP address
- Local IP address or addresses and subnet mask

  Note: In a single IP address service, your ISP will refer to your computer's IP address. However, when your connection is configured with a router, this becomes the router's WAN IP address.
- Primary and secondary domain name server (DNS) IP addresses
- Domain name (usually the same as the ISP's domain name unless you have registered for your own individual domain name)

Note: The default gateway, WAN address and mask, DNS, and domain name are all obtainable via WAN DHCP, if your ISP supports it.

With Network Address Translation

If you are using NAT, you should obtain the following:

- If you are connecting to a remote site using Network Address Translation on your router, your provider will not define the IP address information on your local LAN. You can define this information based on an IP configuration that may already be in place for the existing network. Alternatively, you can use the default IP address range used by the router, where 192.168.1.1 is the default IP address of the router.

Without Network Address Translation

If you are *not* using Network Address Translation, you will need to obtain all of the local LAN IP address information from your ISP and you will need to pay for an IP address for each device on the network.

If you are not using NAT, you should obtain:

- The Ethernet IP address for your Netopia R910
- The Ethernet IP subnet mask for your Netopia R910
- An IP address for each device on your network, in the same network range as the Netopia R910.

Chapter 3

Making the Physical Connections

This section tells you how to make the physical connections to your Netopia R910 Ethernet Router. This section covers the following topics:

Find a location

When choosing a location for the Netopia Router, consider:

- Available space and ease of installation
- Physical layout of the building and how to best use the physical space available for connecting your Netopia Router to the LAN
- Available wiring and jacks
- Distance from the point of installation to the next device (length of cable or wall wiring)
- Ease of access to the front of the unit for configuration and monitoring
- Ease of access to the back of the unit for checking and changing cables
- Cable length and network size limitations when expanding networks

For small networks, install the Netopia R910 near one of the LANs. For large networks, you can install the Netopia R910 in a wiring closet or a central network administration site. In most cases the router will be near the cable or DSL modem which is near the cable or DSL wall outlet. You could pull a line from the wall outlet to a wiring closet if you store the modem and router there.

What you need

Locate all items that you need for the installation.

Included in your router package are:

- The Netopia R910 Ethernet Router
- A power adapter and cord with a mini-DIN8 connector
- Two RJ-45 cables (one for the Ethernet port on your PC; one for the Line port on the router)
- A DB-9 console cable
- A cross-over cable
- The Netopia CD containing an Internet browser, Adobe Acrobat Reader for Windows and Macintosh, ZTerm terminal emulator software and NCSA Telnet for Macintosh, and documentation

You will need:

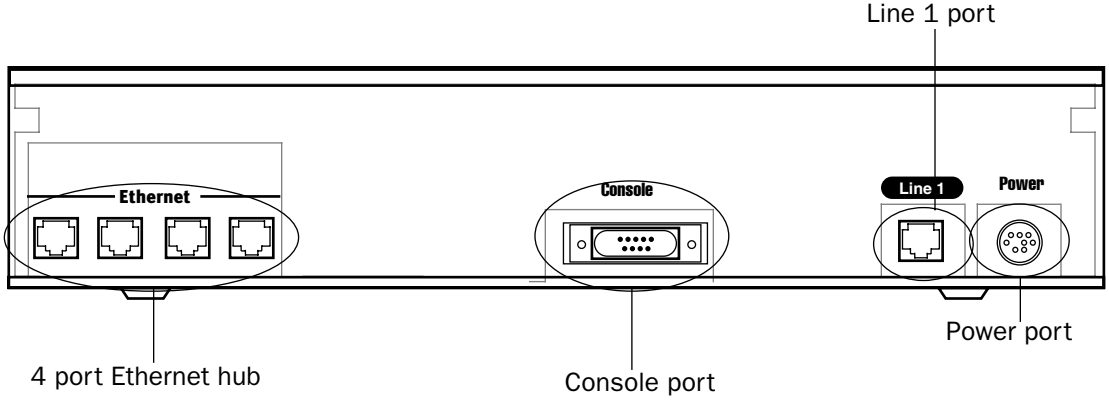
- A Windows 95, 98, 2000, or NT–based PC or a Macintosh computer with Ethernet connectivity for configuring the Netopia R910. This may be built-in Ethernet or an add-on card, with TCP/IP installed and configured. See "Hardware and operating system requirements" on page 5-23.
- An Internet modem such as a cable modem or DSL bridge connected to the appropriate wall outlet for your Internet service source. Your Internet connection device must have a 10Base-T Ethernet port for connecting it to the router's Line port.

Identify the connectors and attach the cables

Identify the connectors and switches on the back panel and attach the necessary Netopia Router cables.

The figure below displays the back of the Netopia R910 Ethernet Router.

Netopia R910 Ethernet Router back panel



1. Connect the mini-DIN8 connector from the power adapter to the power port, and plug the other end into an electrical outlet.

2. Connect one end of one of the RJ-45 cables to the Line 1 port and the other end to your Internet modem's Ethernet port. DO NOT CONNECT IT DIRECTLY TO A TELCO LINE OUTLET.

3. Connect one end of one of the RJ-45 cables to any of the Ethernet hub ports on the router, and the other end to the Ethernet port of your PC.

   If you are connecting the router to an existing Ethernet hub, use a cross-over cable.

   You should now have: the power adapter plugged in; the Ethernet cable connected between the router and your computer; and the Line cable connected between the router and your Internet modem.

Netopia R910 Ethernet Router back panel ports

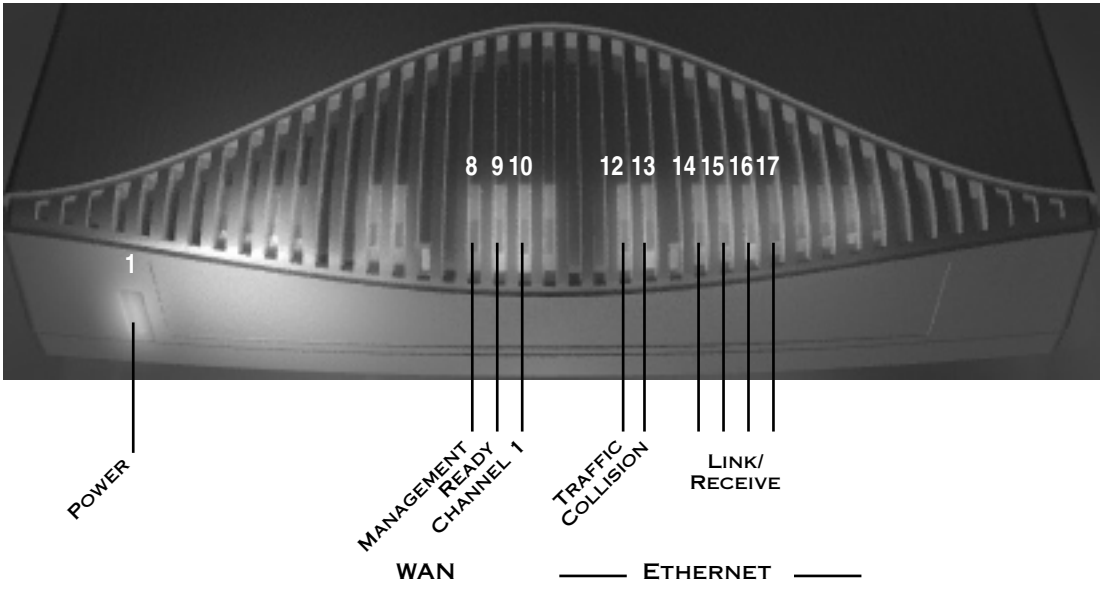
The following table describes all the Netopia R910 Ethernet Router back panel ports.

Port	Description
Power port	A mini-DIN8 power adapter cable connection.
Line port	The dedicated Ethernet port for your connection to your Internet connection device's Ethernet port.
Console port	A DB-9 console port for a direct serial connection to the console screens. You can use this if you are an experienced user. See "Connecting a console cable to your router" on page 6-33.
4-port Ethernet hub	Four Ethernet jacks. You will use one of these to configure the Netopia R910. For a new installation, use the Ethernet connection. Alternatively, you can use the console connection to run console-based management using a direct serial connection. You can either connect your computer directly to any of the Ethernet ports on the router, or connect both your computer and the router to an existing Ethernet hub on your LAN.

Netopia R910 Ethernet Router status lights

The figure below represents the Netopia R910 status light (LED) panel.

Netopia R910 LED front panel



The following table summarizes the meaning of the various LED states and colors:

When this happens...	the LEDs...
Power is on	1 is **green**.
Data is transmitted or received	8 flashes **orange**.
The WAN interface is operational	9 is **green**.
The WAN interface is inactive	9 is **off**.
The WAN interface detects a failure after line activation	9 flashes **red**.
Calls are setting up	10 flashes **green**.
Data calls connect	10 is **green**.
The line is carrying data traffic	10 flashes **orange**.
The Ethernet port is connected to the LAN	14, 15, 16, and 17 are **green**.
There is activity on the respective Ethernet ports	14, 15, 16, and 17 flash **green**.
Note: The Channel 2 LED and the unlabeled LEDs are not used.	

Chapter 4

Connecting to Your Local Area Network

This chapter describes how to physically connect the Netopia R910 to your local area network (LAN). Before you proceed, make sure the Netopia R910 is properly configured. You can customize the router's configuration for your particular LAN requirements using console-based management (see "Console-Based Management" on page 6-31).

This section covers the following topics:

Overview

You can connect the Netopia R910 to an IP network that uses Ethernet.

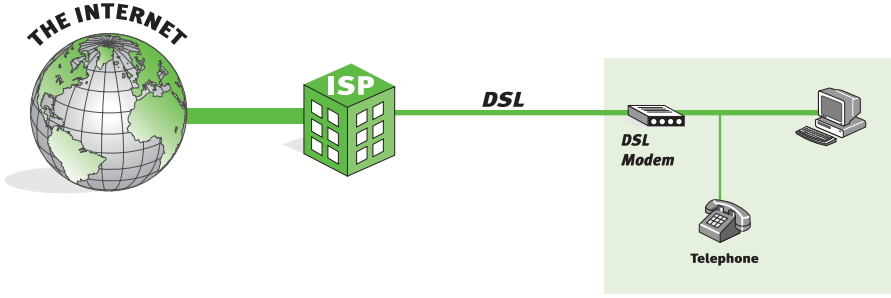
Network Model

The following diagrams illustrate network models for typical deployments of the Netopia R910 Ethernet Router as an Internet access device.

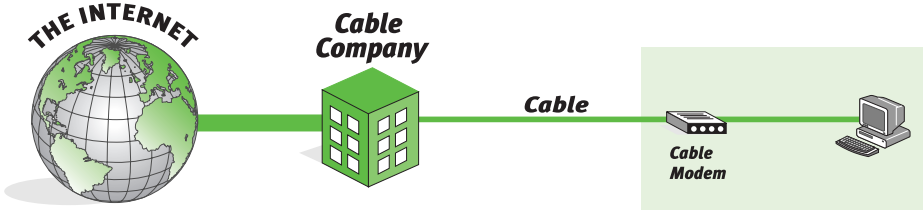
Before

With a DSL or cable modem, you can connect a single computer to the Internet.

using a DSL modem



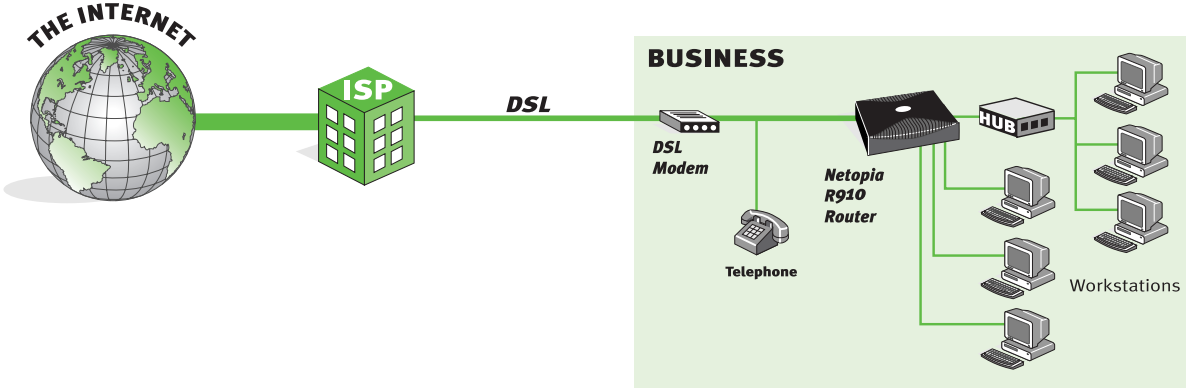
using a cable modem



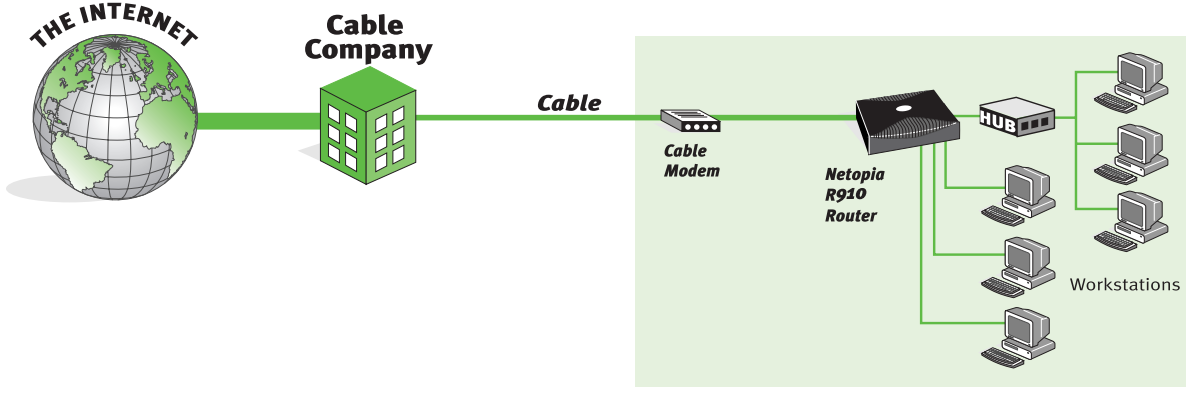
After

Using the Netopia R910 Ethernet Router, you can connect multiple computers to the Internet with a single user account.

using a DSL modem with a Netopia R910



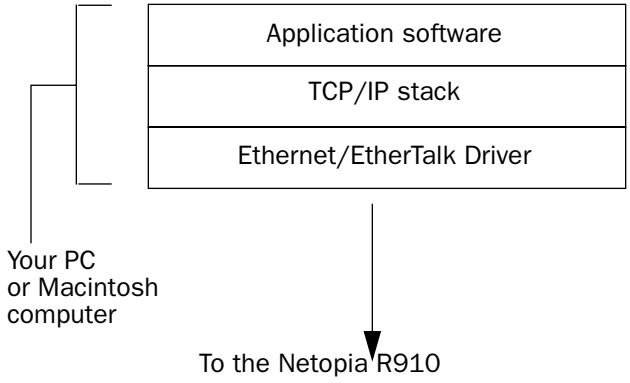
using a cable modem with a Netopia R910



While this network model is typical, other network models are possible. For example, you may choose to attach the Ethernet WAN port to an external Ethernet hub connected to a number of workstations.

Readying computers on your local network

PC and Macintosh computers must have certain components installed before they can communicate through the Netopia R910. The following illustration shows the minimal requirements for a typical PC or Macintosh computer.



Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora e-mail client and the Web browsers Microsoft Internet Explorer and Netscape Navigator.

TCP/IP stack: This is the software that lets your PC or Macintosh communicate using Internet protocols. TCP/IP stacks must be configured with some of the same information you used to configure the Netopia R910. There are a number of TCP/IP stacks available for PC computers. Windows 95 includes a built-in TCP/IP stack. See "Configuring TCP/IP on Windows 95 or 98" on page 5-24. Macintosh computers use either MacTCP or Open Transport. See "Configuring TCP/IP on a Macintosh Computer" on page 5-26.

Ethernet: Ethernet hardware and software drivers enable your PC or Macintosh computer to communicate on the LAN.

EtherTalk: This is an AppleTalk protocol used over Ethernet.

Once the Netopia R910 is properly configured and connected to your LAN, PC and Macintosh computers that have their required components in place will be able to connect to the Internet or other remote IP networks.

Connecting to an Ethernet network

The Netopia R910 supports Ethernet connections through its four Ethernet ports. The router automatically detects which Ethernet port is in use.

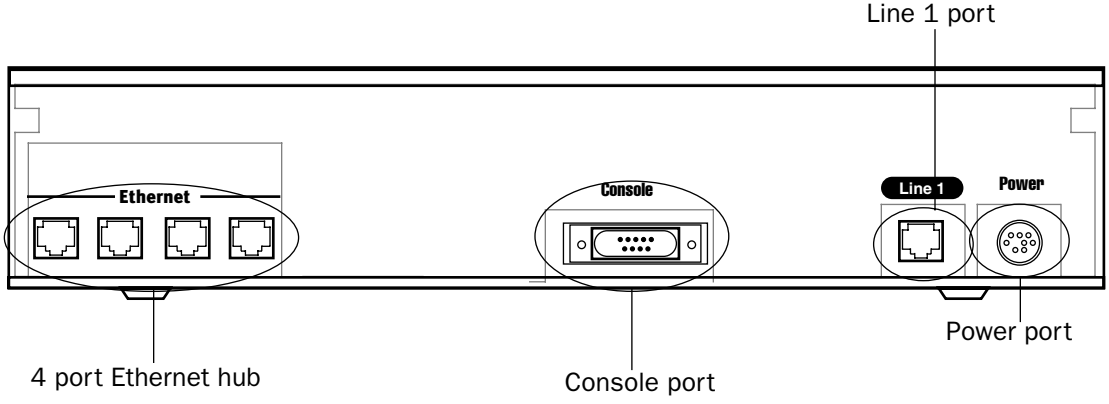
You can connect 10Base-T networks to the Netopia R910. The following table displays some important attributes of these connections.

Attribute	10Base-T
Max. length of backbone, branch, or end to end (cable length)	330 feet (100 meters)
Cable type	Twisted pair (10Base-T)
Netopia R910 port used	Ethernet
Other restrictions	No daisy chain

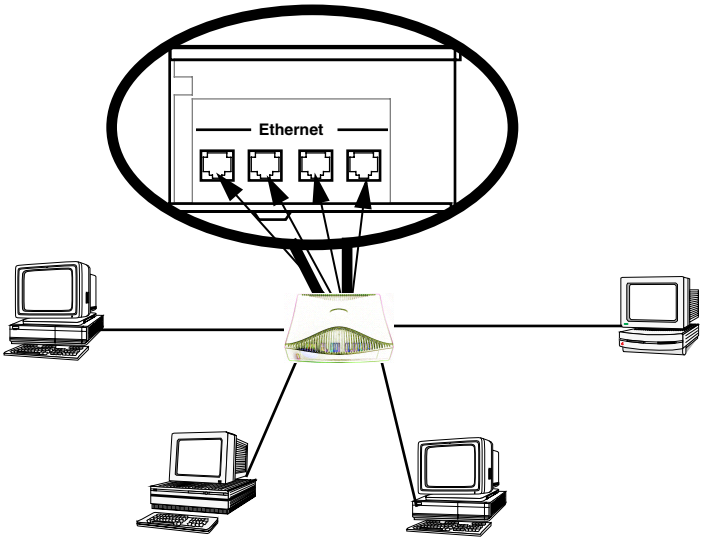
10Base-T

You can connect a standard 10Base-T Ethernet network to the Netopia R910 using any of its available Ethernet ports.

Netopia R910 Ethernet Router back panel



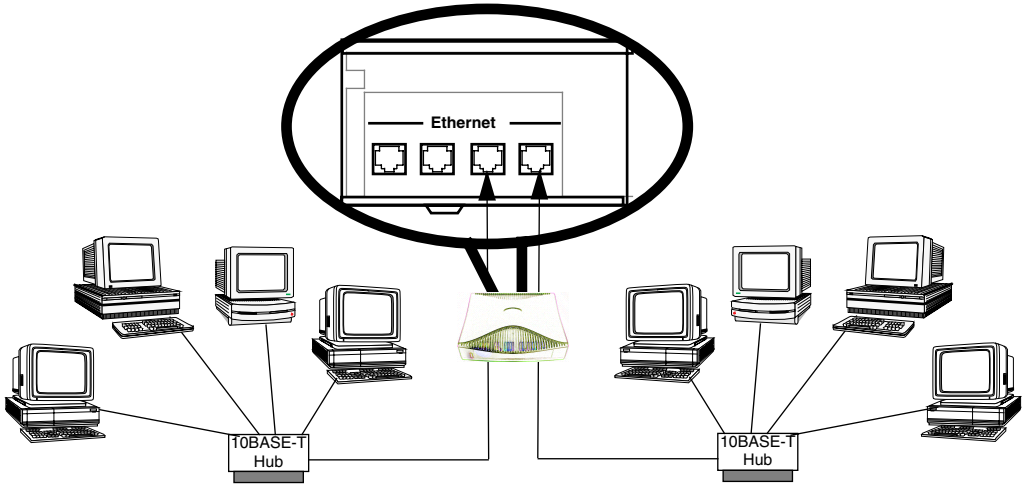
The Netopia R910 in a 10Base-T network



To connect your 10Base-T network to the Netopia R910 through an Ethernet port, use a 10Base-T cable with RJ-45 connectors.

If you have more than four devices to connect, you can attach additional devices using a 10Base-T hub, using a cross-over cable.

The Netopia R910 in a 10Base-T network with a hub



Chapter 5

Configuring TCP/IP

Be sure the computer you use to configure your Netopia R910 has TCP/IP software and hardware properly configured to work with a router and the network service provider you will be using. Typically, this means that you will have your computer set up to accept a dynamically assigned IP address from the router, although other options are possible. This chapter is a general guide to configuring TCP/IP connectivity for your PC or Macintosh. Consult your computer's documentation for more detail.

This section covers the following topics:

If after following the instructions in this section you are having difficulties configuring the router, see Appendix A, "Troubleshooting."

Hardware and operating system requirements

Before you can configure your router make sure your computer meets the following requirements:

	PC	Macintosh
System software	Windows 95, 98, or NT operating system	MacOS 7.5 or later (minimum system version: 7.5)
Connectivity software	TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Windows 95 or 98" on page 5-24	MacTCP or Open Transport TCP/IP must be installed and properly configured. See "Configuring TCP/IP on a Macintosh Computer" on page 5-26.
Connectivity hardware	Ethernet card (10Base-T)	Either built-in Ethernet or a third-party Ethernet card (10Base-T)

Configuring TCP/IP on Windows 95 or 98

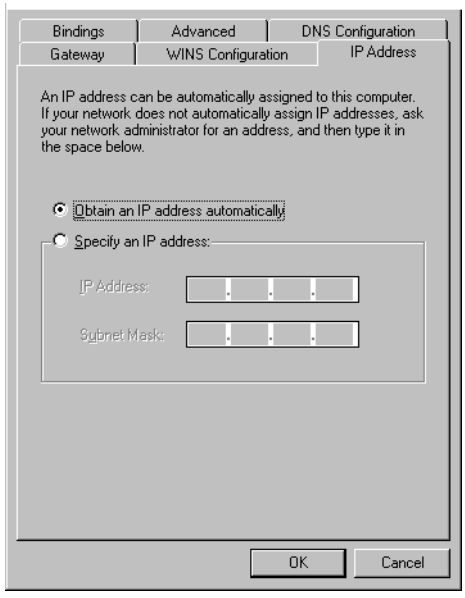
Be sure TCP/IP is installed and configured on your Windows computer. The following is a quick guide to configuring TCP/IP for Windows machines. Configuring TCP/IP in a Windows machine requires the following:

- An Ethernet card (also known as a network adapter)
- The TCP/IP protocol must be "bound" to the adapter or card

Dynamic configuration (recommended)

The easiest configuration method is to accept the dynamic IP address assigned by your router. Dynamic Host Configuration Protocol (DHCP), which enables dynamic addressing, is enabled by default on the router.

1. Go to Start Menu/Settings/Control Panels and double click the Network icon. From the **Network** components list, select the **Configuration** tab.
2. Select TCP/IP–>Your Network Card. Then select **Properties**. In the TCP/IP Properties screen (shown at right), select the **IP Address** tab. Click "Obtain an IP Address automatically."
3. Click **OK** in this window, and the next window. When prompted, reboot the computer.



Static configuration (optional)

If you are manually configuring from a fixed or static IP address, perform the following:

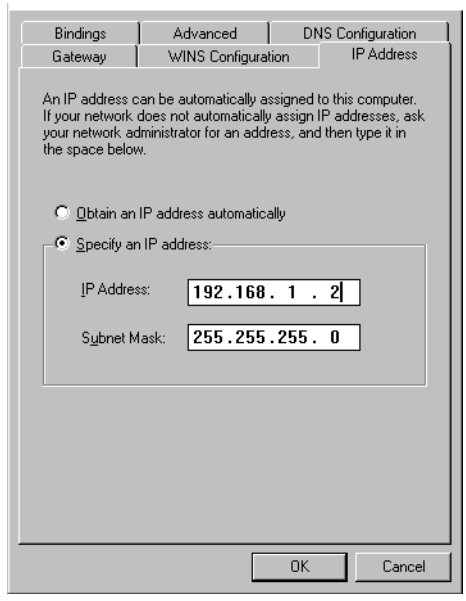
1. Go to Start Menu/Settings/Control Panels and double click the **Network** icon. From the Network components list, select the **Configuration** tab.
2. Select TCP/IP–>Your Network Card. Then select **Properties**. In the TCP/IP Properties screen (shown at right), select the **IP Address** tab. Click "Specify an IP Address." Enter the following:
   IP Address: 192.168.1.2
   Subnet Mask: 255.255.255.0
   Your ISP or network administrator may ask you to use a different IP address and subnet mask.
3. Click on the **Gateway** tab (shown at right). Under New gateway, enter 192.168.1.1. Click **Add**. This is the address that is assigned to the Netopia R910.
4. Click on the **DNS Configuration** tab. Click "Enable DNS." Enter the following information:

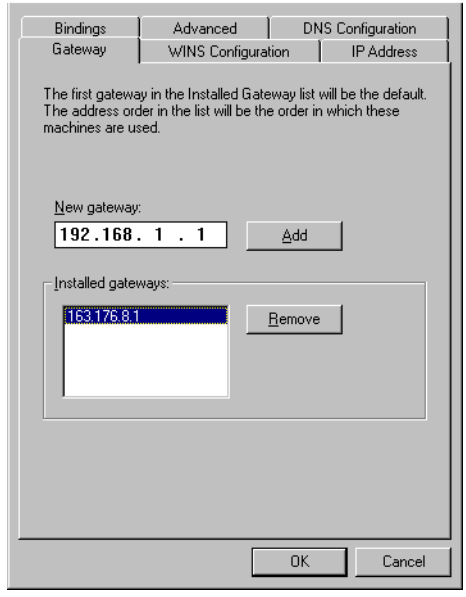
   Host: Type the name you want to give to this computer.

   Domain: Type your domain name. If you don't have a domain name, type your ISP's domain name; for example, netopia.com.

   DNS Server Search Order: Type the primary DNS IP address given to you by your ISP. Click **Add**. Repeat this process for the secondary DNS.

   Domain Suffix Search Order: Enter the same domain name you entered above.
5. Click **OK** in this window, and the next window. When prompted, reboot the computer.





Note: More details about Windows 95 TCP/IP configuration (including dial-up) can be found in Technote NIR_027, "Windows 95 TCP/IP Properties and the Netopia Router," located on the Netopia Web site.

Configuring TCP/IP on a Macintosh Computer

The following is a quick guide to configuring TCP/IP for MacOS computers. Configuring TCP/IP on a Macintosh computer requires the following:

- You must have either Open Transport or MacTCP installed.

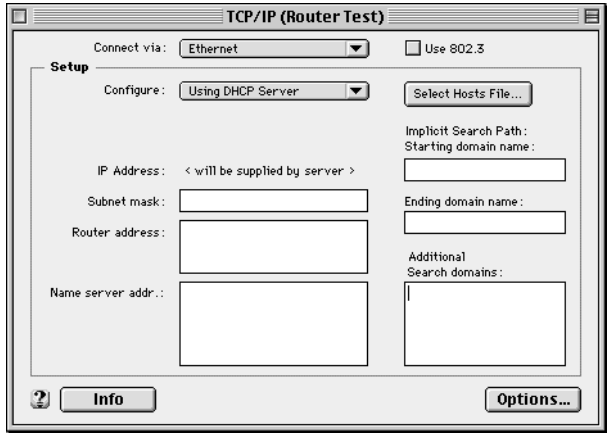
  Note: If you want to use the Dynamic Host Configuration Protocol (DHCP) server built into your Netopia R910 to assign IP addresses to your Macintoshes, you must be running Open Transport. You can have your Netopia R910 dynamically assign IP addresses using MacTCP; however, to do so requires that the optional AppleTalk kit be installed and this can only be done after the router is configured.

- You must have built-in Ethernet or a third-party Ethernet card and its associated drivers installed in your Macintosh.

Dynamic configuration (recommended)

The easiest configuration method is to accept the dynamic IP address assigned by your router. DHCP, which enables dynamic addressing, is enabled by default on the router.

1. Go to the Apple Menu. Select **Control Panels** and then **TCP/IP**.
2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Basic** and click **OK**.
3. In the TCP/IP window, select "Connect via: Ethernet" and "Configure: Using DHCP Server."



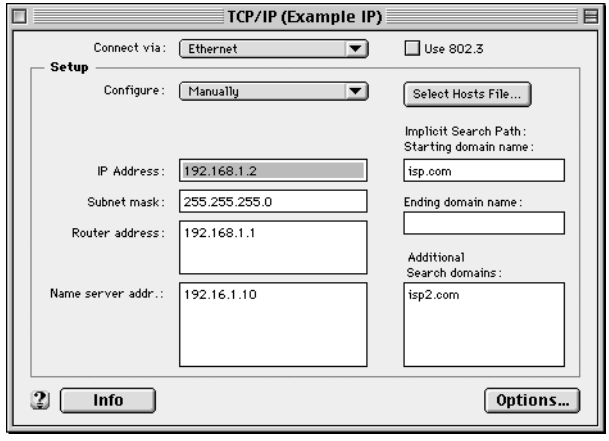
Static configuration (optional)

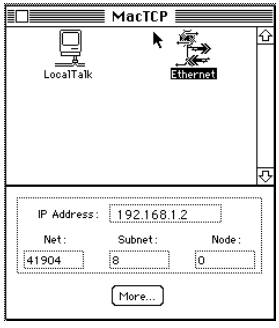
If you are manually configuring from a fixed or static IP address, then perform the following:

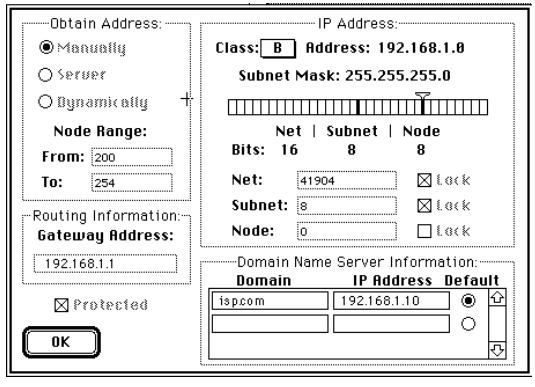
1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP** or **MacTCP**.
2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**. In the MacTCP window, select **Ethernet** and click the **More** button.
3. In the TCP/IP window or in the MacTCP/More window, select or type information into the fields as shown in the table at right.
4. Close the TCP/IP or MacTCP control panel and save the settings.
5. If you are using MacTCP, you must restart the computer. If you are using Open Transport, you do not need to restart.

   These are the only fields you need to modify in this screen.

Option:	**Select/Type:**
Connect via:	Ethernet
Configure:	Manually
IP Address:	192.168.1.2
Subnet mask:	255.255.255.0
Router address:	192.168.1.1
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP







Dynamic configuration using MacIP (optional)

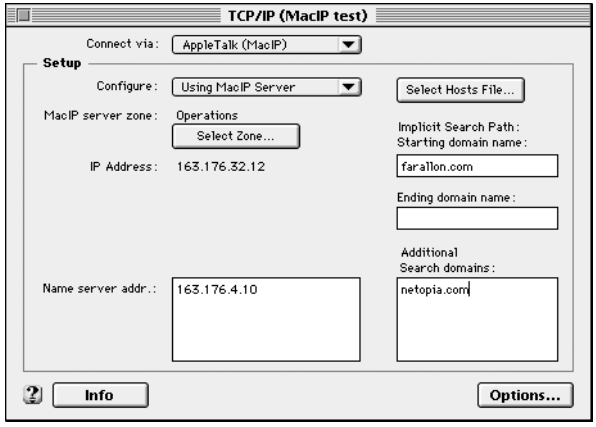
If you want to use MacIP to dynamically assign IP addresses to the Macintosh computers on your network you must install the optional AppleTalk feature set kit.

Note: You cannot use MacIP dynamic configuration to configure your Netopia R910 Ethernet to Ethernet Router because you must first configure the router in order to enable AppleTalk.

Once the AppleTalk kit is installed, you can configure your Macintoshes for MacIP. To configure dynamically using MacIP, perform the following:

Using Open Transport TCP/IP

1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP**.
2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**.



3. In the TCP/IP window, select or type information into the fields as shown in the following table.

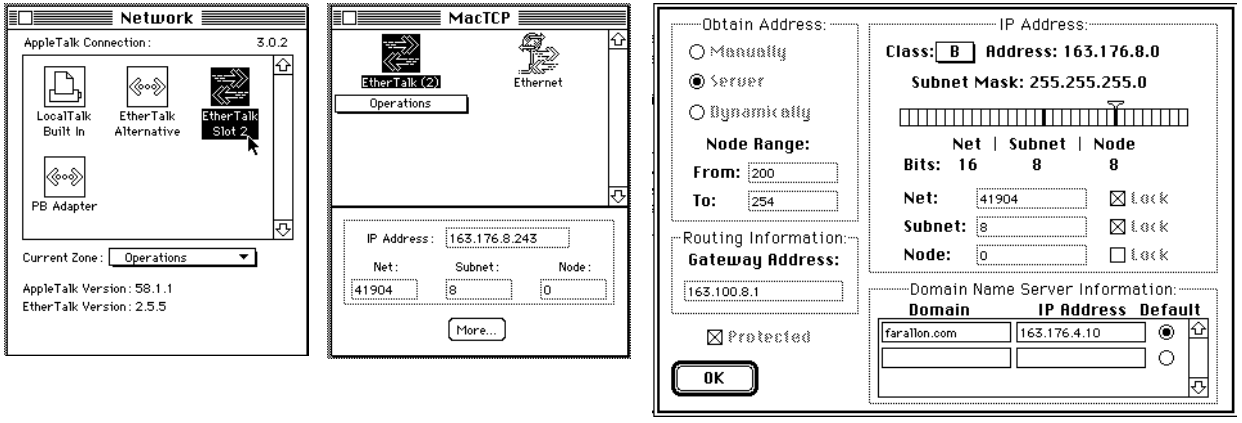
TCP/IP Option:	Select/ Type:
Connect via:	AppleTalk (MacIP)
Configure:	Using MacIP server
MacIP Server zone:	(select available zone)
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

4. Close the TCP/IP control panel and save the settings.

   These are the only fields you need to modify in these screens.

Using Classic Networking (MacTCP)

1. Go to the Apple Menu. Select **Control Panels** and then **Network**.
2. In the Network window, select **EtherTalk**.



3. Go back to the Apple menu. Select **Control Panels** and then **MacTCP**.
4. Select **EtherTalk**.

   From the pull-down menu under EtherTalk, select an available zone; then click the **More** button.

   In the MacTCP/More window select the **Server** radio button. If necessary, fill in the Domain Name Server Information given to you by your administrator.
5. Restart the computer.

   These are the only fields you need to modify in these screens.

Note: More information about configuring your Macintosh computer for TCP/IP connectivity through a Netopia R910 can be found in Technote NIR_026, “Open Transport and Netopia Routers,” located on the Netopia Web site.

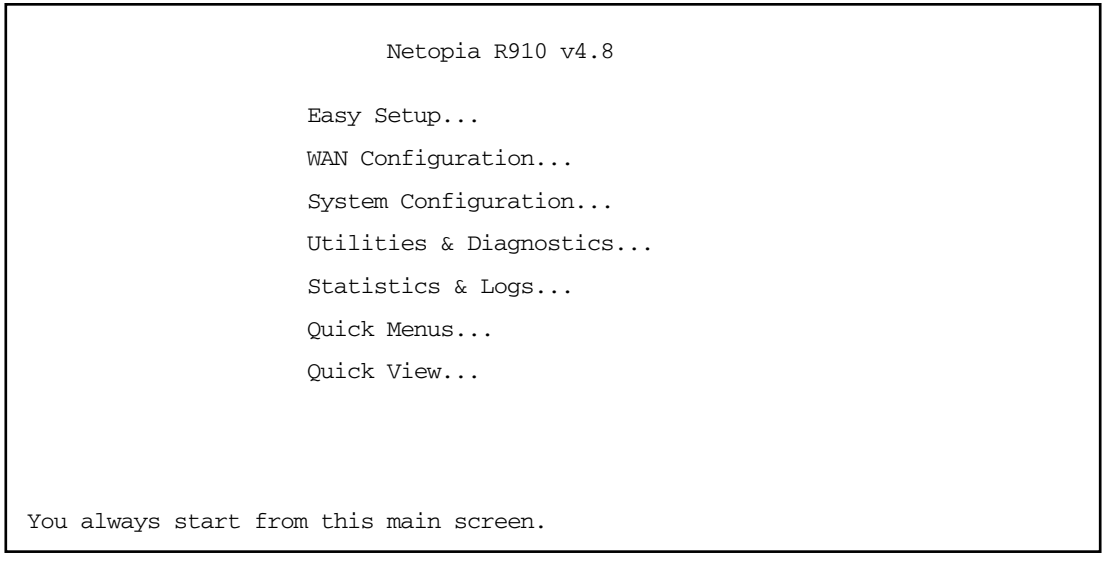
Chapter 6

Console-Based Management

Console-based management is a menu-driven interface for the capabilities built in to the Netopia R910. Console-based management provides access to a wide variety of features that the router supports. You can customize these features for your individual setup. This chapter describes how to access the console-based management screens.

This section covers the following topics:

Console-based management screens contain seven entry points to the Netopia Router configuration and monitoring features. The entry points are displayed in the Main Menu shown below:



- The **Easy Setup** menus display and permit changing the values contained in the default WAN and IP configuration. Experienced users can use Easy Setup to initially configure the router directly through a console session.

  Easy Setup menus contain up to five descendant screens for viewing or altering these values. The number of screens depends on whether you have optional features installed.

- The **WAN Configuration** menu displays and permits changing your WAN and IP configuration(s) and default profile, and configuring or reconfiguring the manner in which you may be using the router to connect to

more than one service provider or remote site.

- The **System Configuration** menus display and permit changing:
  - Network protocols setup. See Chapter 9, "IP Setup and Network Address Translation."
  - Filter sets (firewalls). See "About filters and filter sets" on page 13-126.
  - IP address serving. See "IP address serving" on page 9-66.
  - Date and time. See "Date and time" on page 8-47.
  - Console configuration. See "Connecting a console cable to your router" on page 6-33.
  - SNMP (Simple Network Management Protocol). See "SNMP" on page 12-118.
  - Security. See Chapter 13, "Security."
  - Upgrade feature set. See "Upgrade feature set" on page 8-48.
- The **Utilities & Diagnostics** menus provide a selection of seven tools for monitoring and diagnosing the router's behavior, as well as for updating the firmware and rebooting the system. See Chapter 14, "Utilities and Diagnostics," for detailed information.
- The **Statistics & Logs** menus display a selection of tables and device logs that show information about your router, your network and their history. See Chapter 12, "Monitoring Tools," for detailed information.
- The **Quick Menus** screen is a shortcut entry point to a wide variety of the most commonly used configuration menus that are accessed through the other menu entry points.
- The **Quick View** menu displays at a glance current real-time operating information about your router. See "Quick View status overview" on page 12-109 for detailed information.

Connecting through a Telnet session

Features of the Netopia R910 can be configured through the console screens.

Before you can access the console screens through Telnet, you must have:

- A network connection locally to the router or IP access to the router.

  Note: Alternatively, you can have a direct serial console cable connection using the provided console cable for your platform (PC or Macintosh) and the Console port on the back of the router. For more information on attaching the console cable, see "Connecting a console cable to your router" on page 6-33.
- Telnet software installed on the computer you will use to configure the router

Configuring Telnet software

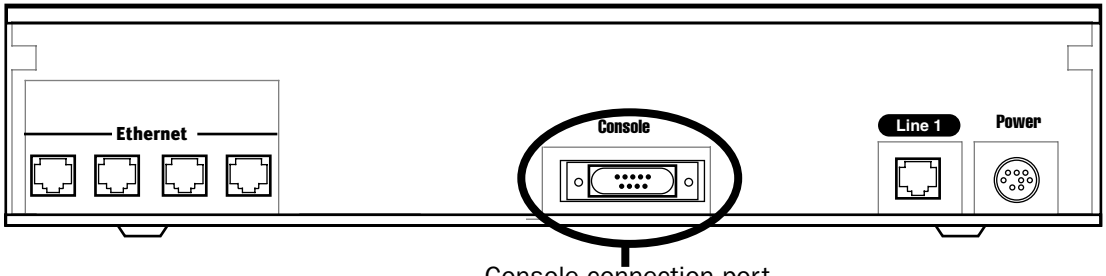
If you are configuring your router using a Telnet session, your computer must be running a Telnet software program.

- If you connect a PC with Microsoft Windows, you can use a Windows Telnet application or simply run Telnet from the Start menu.
- If you connect a Macintosh computer, you can use the NCSA Telnet program supplied on the Netopia R910 CD. You install NCSA Telnet by simply dragging the application from the CD to your hard disk.

Connecting a console cable to your router

You can perform all of the system configuration activities for your Netopia R910 through a local serial console connection using terminal emulation software, such as HyperTerminal provided with Windows95 on the PC, or ZTerm, included on the Netopia CD, for Macintosh computers.

The Netopia R910 back panel has a connector labeled “Console” for attaching the Router to either a PC or Macintosh computer via the serial port on the computer. (On a Macintosh computer, the serial port is called the Modem port or Printer port.) This connection lets you use the computer to configure and monitor the Netopia R910 via the console screens.



Console connection port
DB-9 (male)

To connect the Netopia R910 to your computer for serial console communication, use the supplied console cable.

If you connect a PC with Microsoft Windows 95 or NT, you can use the HyperTerminal application bundled with the operating system.

If you connect a Macintosh computer, you can use the ZTerm terminal emulation program on the supplied CustomerCare CD.

Launch your terminal emulation software and configure the communications software for the values shown in the table below. These are the default communication parameters that the Netopia R910 uses.

Parameter	Suggested Value
Terminal type	**PC**: ANSI-BBS **Mac**: ANSI, VT-100, or VT-200
Data bits	8
Parity	None
Stop bits	1
Speed	Options are: 9600, 19200, or 38400 bits per second
Flow Control	None
Note: The router firmware contains an autobaud detection feature. If you are at any screen on the serial console, you can change your baud rate and press Return (HyperTerminal for the PC requires a disconnect). The new baud rate is displayed at the bottom of the screen.	

Navigating through the console screens

Use your keyboard to navigate the Netopia R910's configuration screens, enter and edit information, and make choices. The following table lists the keys to use to navigate through the console screens.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
To set a change to a selected item or open a pop-up menu of options for a selected item like entering an upgrade key	Return or Enter
Change a toggle value (Yes/No, On/Off)	Tab
Restore an entry or toggle value to its previous value	Esc
Move one item up	Up arrow or Control + o
Move one item down	Down arrow or Control +k
Display a dump of the device event log	Control + e
Display a dump of the WAN event log	Control + f
Refresh the screen	Control + L
Go to topmost selectable item	<
Go to bottom right selectable item	>

Chapter 7

Easy Setup

This chapter describes how to use the Easy Setup console screens on your Netopia R910 Ethernet Router. After completing the Easy Setup console screens, your router will be ready to connect to the Internet or another remote site.

This chapter covers the following topics:

Easy Setup console screens

Using three Easy Setup console screens, you can:

- Define your Wide Area Network (WAN) connection for your router to connect to your ISP or remote location
- Set up IP addresses and IP address serving
- Password–protect configuration access to your Netopia R910 Ethernet Router

Accessing the Easy Setup console screens

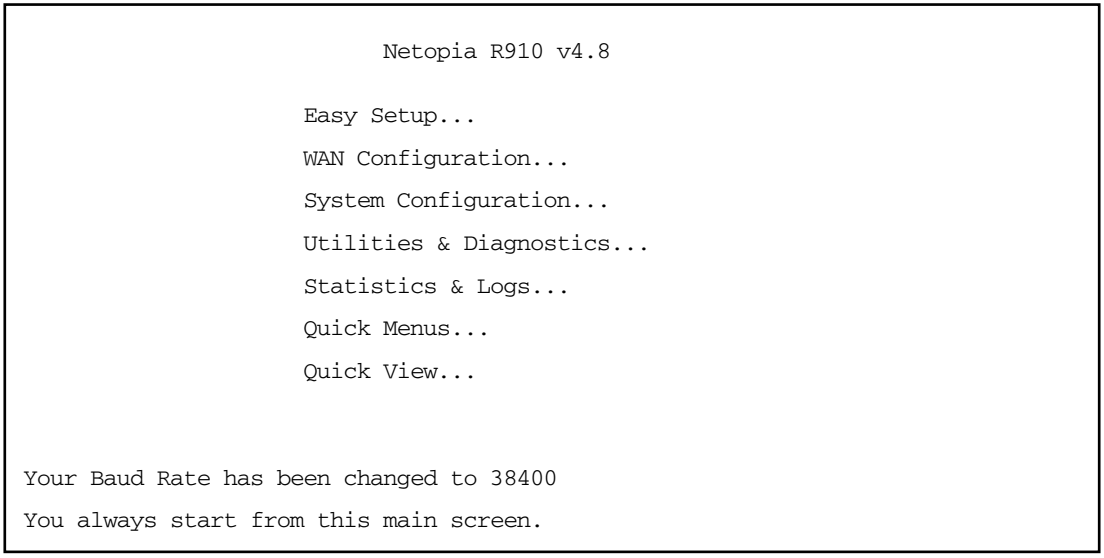
To access the console screens, Telnet to the Netopia Router over your Ethernet network, or physically connect with a serial console cable and access the Netopia Router with a terminal emulation program. See "Connecting through a Telnet session" on page 6-32 or "Connecting a console cable to your router" on page 6-33.

Note: Before continuing, make sure you have the information that your telephone service provider, ISP, or network administrator has given you for configuring the Netopia Router.

The Netopia Router's first console screen, Main Menu, appears in the terminal emulation window of the attached PC or Macintosh computer when

- The Netopia Router is turned on
- The computer is connected to the Netopia Router
- The Telnet or terminal emulation software is running and configured correctly

A screen similar to the following Main Menu appears:



If you do not see the Main Menu, verify that:

- The computer used to view the console screen has its serial port connected to the Netopia R910's Console port or an Ethernet connection to one of its Ethernet ports. See "Connecting a console cable to your router" on page 6-33 or "Connecting through a Telnet session" on page 6-32.
- The Telnet or terminal emulation software is configured for the recommended values.
- If you are connecting via the Console port, your computer's serial port is not being used by another device, such as an internal modem, or an application. Turn off all other programs (other than your terminal emulation program) that may be interfering with your access to the port.
- You have entered the correct password, if necessary. Your Netopia R910's console access may be password protected from a previous configuration. See your system administrator to obtain the password.

  See Appendix A, "Troubleshooting," for more suggestions.

Quick Easy Setup connection path

This section may be all you need to do to configure your Netopia R910 Ethernet Router to connect to the Internet.

If your ISP supports DHCP

Your Netopia R910 Ethernet Router comes preconfigured with the ability to accept an IP address dynamically assigned by your ISP. To do this, it acts as a Dynamic Host Configuration Protocol client to your ISP's DHCP server. This means that each time you power the Router on when it is connected to the Internet connection line, it configures itself with IP address settings without any input on your part. If your ISP supports this method, skip these instructions and go to Chapter 4, "Connecting to Your Local Area Network." You don't need to do anything else. This is the true Plug-and-Play solution.

If your ISP doesn't support DHCP

Some ISPs may not be running a DHCP server. In this case, they may simply assign your router a Static IP Address and will supply you with several values for you to enter into the Router. The ISP will provide the values shown below:

Local WAN IP Address	
Local WAN IP Mask	
Default IP Gateway	
Domain Name	
Primary Domain Name Server	
Secondary Domain Name Server	

(You can record these values; print this page and use the spaces above.)

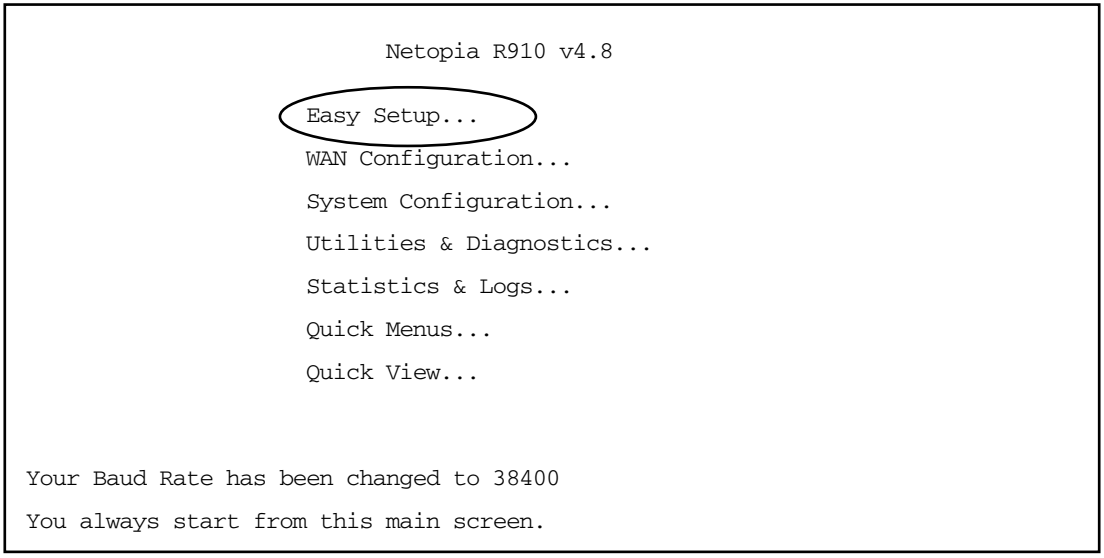
If your ISP assigns your Router a Static IP address, do the following:

1. From the computer connected to your router, as described in the section "Identify the connectors and attach the cables" on page 3-14, open a Telnet session to 192.168.1.1 to bring up the **Main Menu**.

   If you don't know how to do this, see "Connecting through a Telnet session" on page 6-32.

   Alternatively, you can connect the console cable and open a direct serial console connection, using a terminal emulator program. See "Connecting through a Telnet session" on page 6-32.

The Main Menu appears.



2. Select the first item on the Main Menu list, **Easy Setup**. Press Return to bring up the Easy Setup menu screen.
3. Press the Down arrow key until the editable field labelled **Local WAN IP Address** is highlighted.
4. Type the IP Address your ISP gave you. Press Return. The next field **Local WAN IP Mask** will appear.
5. Type the Subnet Mask your ISP gave you. Press Return.
6. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return to bring up the next screen.
7. Press the Down arrow key until the editable field labelled **Domain Name** is highlighted.
8. Type the Domain Name your ISP gave you. Press Return. The next field **Primary Domain Name Server** will be highlighted.
9. Type the Primary Domain Name Server address your ISP gave you. Press Return. A new field **Secondary Domain Name Server** will appear. If your ISP gave you a secondary domain name server address, enter it here. Press Return until the next field **Default IP Gateway** is highlighted.
10. Enter the Default IP Gateway address your ISP gave you. Press Return.
11. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return.
12. Do this again, through the next two screens until you reach **RESTART DEVICE**. When RESTART DEVICE is highlighted, press Return. When prompted, select **CONTINUE**, and press Return.

The router will restart and your configuration settings will be activated. You can then Exit or Quit your Telnet application.

For more Easy Setup options see "More Easy Setup options" on page 7-39.

More Easy Setup options

You always begin Easy Setup by selecting **Easy Setup** in the Main Menu, then pressing Return.

The WAN Ethernet Configuration screen appears.

```
                        WAN Ethernet Configuration

          PPOE:                                 Yes
          Address Translation Enabled:          Yes
          Local WAN IP Address:                 0.0.0.0









          TO MAIN MENU                          NEXT SCREEN

Set up the basic IP attributes of your Ethernet Module in this screen.
```

WAN Ethernet Configuration

The WAN Ethernet Configuration screen is where you configure the parameters that control the Netopia R910's connection to a specific remote destination, usually your ISP or a corporate site.

1. To enable address translation, toggle **Address Translation Enabled** to **Yes** (the default). For more information on Network Address Translation, see Chapter 9, "IP Setup and Network Address Translation."

   Address Translation Enabled allows you to specify whether or not the router performs Network Address Translation (NAT) on the Ethernet WAN port. NAT is enabled by default.

2. To *manually* configure an IP address for use on the Ethernet WAN port, select **Local WAN IP Address** and enter the IP address you want to use.

   Otherwise, accept the default value 0.0.0.0. If you accept the default, the Netopia R910 Ethernet Router will act as a DHCP client on the Ethernet WAN port and attempt to acquire an address from a DHCP server. By default, the router acts as a DHCP client on the Ethernet WAN port and obtains its IP address and subnet mask from the DHCP server.

3. A new field **Local WAN IP Mask** (not shown) becomes visible only if you have configured a non-zero Ethernet IP address. If you have configured a non-zero Ethernet IP address, enter an appropriate subnet mask.

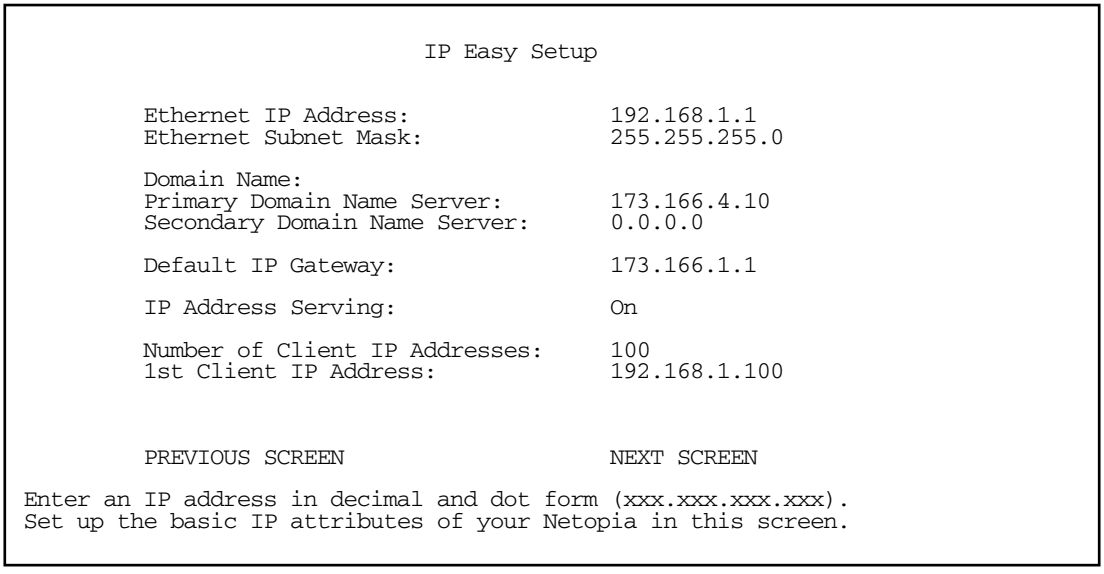
4. Select **NEXT SCREEN** and press Return. The IP Easy Setup screen appears.

IP Easy Setup

The IP Easy Setup screen is where you enter information about your Netopia Router's:

- Ethernet IP address
- Ethernet Subnet mask
- Domain Name
- Domain Name Server IP address
- Default gateway IP address
- Whether to serve IP addresses or not

Consult with your network administrator to obtain the information you will need. For more information about setting up IP, see "IP Setup and Network Address Translation" on page 9-51.



1. Select **Ethernet IP Address** and enter the first IP address from the IP address range your ISP has given you. This will be the Netopia Router's IP address.

   If Network Address Translation is enabled in Easy Setup, the Ethernet IP Address defaults to an address within a range reserved by the Internet address administration authority for use within private networks, 192.168.1.1.

   Because this is a private network address, it should never be directly connected to the Internet. Using NAT for all your WAN and IP configurations will ensure this restriction. See "IP Setup and Network Address Translation" on page 9-51 of this guide for more information.

2. Select **Ethernet Subnet Mask** and enter the subnet mask your ISP has given you. The Ethernet Subnet Mask defaults to a standard class mask derived from the class of the Ethernet IP address you entered in the previous step.

3. Select **Domain Name** and enter the domain name your ISP has given you.

Note: If the Netopia R910's WAN interface is acting as a DHCP client, do not change the default settings for Steps 3, 4, and 5.

4. Select **Primary Domain Name Server** and enter the IP address your ISP has given you. An alternate or **Secondary Domain Name Server** field will appear, where you can enter a secondary DNS IP address if your ISP has given you one.
5. If you do not enter a **Default IP Gateway** value, the router defaults to the remote IP address you entered in Easy Setup. If the Netopia Router does not recognize the destination of any IP traffic, it forwards that traffic to this gateway.

   Do not confuse the remote IP address and the Default IP Gateway's address with the block of local IP addresses you receive from your ISP. You use the local IP addresses for the Netopia R910's Ethernet port and for IP clients on your local network. The remote IP address and the default gateway's IP address should point to your ISP's router.
6. Toggle **IP Address Serving** to **On** or **Off**.
7. Select **NEXT SCREEN** and press Return. The Easy Setup Security Configuration screen appears.

Easy Setup Security Configuration

The Easy Setup Security Configuration screen lets you password-protect your Netopia R910. Input your **Write Access Name** and **Write Access Password** with names or numbers totaling up to eleven digits.

If you password protect the console screens, you will be prompted to enter the name and password you have specified every time you log in to the console screens. Do not forget your name and password. If you do, you will be unable to access any of the configuration screens.

Additional security features are available. See Chapter 13, "Security."

```
                    Easy Setup Security Configuration

It is strongly suggested that you password-protect configuration access to your
Netopia. By entering a Name and Password pair here, access via serial,
Telnet, SNMP and Web Server will be password-protected.

Be sure to remember what you have typed here, because you will be prompted for
it each time you configure this Netopia.

You can remove an existing Name and Password by clearing both fields below.

          Write Access Name:

          Write Access Password:



          PREVIOUS SCREEN       TO MAIN MENU      RESTART DEVICE

Configure a Configuration Access Name and Password here.
```

The final step in configuring the Easy Setup console screens is to restart the Netopia R910, so that the configuration settings take effect.

1. Select **RESTART DEVICE**. A prompt asks you to confirm your choice.
2. Select **CONTINUE** to restart the Netopia Router and have your selections take effect.

Note: You can also restart the system at any time by using the Restart System utility (see "Restarting the system" on page 14-166) or by turning the Netopia Router off and on with the power switch.

Easy Setup is now complete.

Chapter 8

WAN and System Configuration

Console-based management is a menu-driven interface for the capabilities built in to the Netopia R910. Console-based management provides access to a wide variety of features that the router supports. You can customize these features for your individual setup. This chapter describes how to access the console-based management screens.

This section covers the following topics:

WAN configuration

To configure your Wide Area Network (WAN) connection, navigate to the WAN Configuration screen from the Main Menu and select **WAN Configuration**, then **WAN Ethernet Configuration**.

The WAN Ethernet Configuration screen appears.

```
                    WAN Ethernet Configuration

Address Translation Enabled:        Yes
Local WAN IP Address:               0.0.0.0


NAT Map List...                     Easy-PAT List
NAT Server List...                  Easy-Servers

Filter Set...
Remove Filter Set

Receive RIP:                        Both


Enable PPP over Ethernet:           On

Wan Ethernet MAC Address:           00:00:c5:70:03:4a
```

- **Address Translation Enabled** allows you to specify whether or not the router performs Network Address Translation (NAT) on the Ethernet WAN port. NAT is enabled by default.
- **Local WAN IP Address** allows you to manually configure an IP address for use on the Ethernet WAN port. The value 0.0.0.0 indicates that the device will act as a DHCP client on the Ethernet WAN port and attempt to acquire an address from a DHCP server. By default, the router acts as a DHCP client on the Ethernet WAN port.
- **Local WAN IP Mask** allows you to manually configure an IP subnet mask for use on the Ethernet WAN port. This item is visible only if you have configured a non-zero Ethernet IP Address; otherwise, the router obtains a subnet mask via DHCP.
- The **Filter Set** pop-up allows you to associate an IP filter set with the Ethernet WAN port. See "About filters and filter sets" on page 13-126.
- **Remove Filter Set** allows you to remove a previously associated filter set.
- The **Receive RIP** pop-up controls the reception and transmission of Routing Information Protocol (RIP) packets on the Ethernet WAN port. The default is Both. The Transmit RIP pop-up is hidden if NAT is enabled.

  Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia R910 needs to recognize. Set to "Both" (the default) the Netopia R910 will accept information from either RIP v1 or v2 routers. Alternatively, select **Receive RIP** and select **v1** or **v2** from the popup menu. With Receive RIP set to "v1," the Netopia R910's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to "v2," the Netopia R910 will accept routing information provided by RIP packets from other routers that use different subnet masks.

  If you want the Netopia R910 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia R910 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia R910 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia R910 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

System configuration screens

You can connect to the Netopia R910's system configuration screens in either of two ways:

- By using Telnet with the Router's Ethernet port IP address
- Through the console port, using a local terminal (see "Connecting a console cable to your router" on page 6-33)

You can also retrieve the Netopia R910's configuration information and remotely set its parameters using the Simple Network Management Protocol (see "SNMP" on page 12-118).

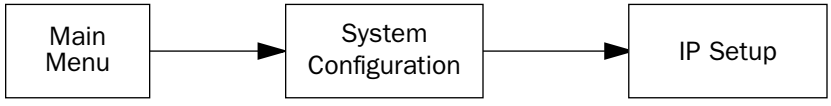
Open a Telnet connection to the router's IP address; for example, "192.168.1.1."

The console screen will open to the **Main Menu**, similar to the screen shown below:

```
                        Netopia R910 v4.8

                    Easy Setup...
                    WAN Configuration...
                    System Configuration...
                    Utilities & Diagnostics...
                    Statistics & Logs...
                    Quick Menus...
                    Quick View...



You always start from this main screen.
```

Navigating through the system configuration screens

To help you find your way to particular screens, some sections in this guide begin with a graphical path guide similar to the following example:



This particular path guide shows how to get to the Network Protocols Setup screens. The path guide represents these steps:

1. Beginning in the Main Menu, select **System Configuration** and press Return. The System Configuration screen appears.
2. Select **IP Setup** and press Return. The IP Setup screen appears.

To go back in this sequence of screens, use the Escape key.

System configuration features

The Netopia R910 Ethernet Router's default settings may be all you need to configure your Netopia R910. Some users, however, require advanced settings or prefer manual control over the default selections. For these users, the Netopia R910 provides system configuration options.

To help you determine whether you need to use the system configuration options, review the following requirements. If you have one or more of these needs, use the system configuration options described in later chapters.

- System configuration of dynamic IP address distribution through DHCP or BootP
- Greater network security through the use of filters

To access the system configuration screens, select **System Configuration** in the Main Menu, then press Return.

The System Configuration menu screen appears:

```
                          System Configuration


                    IP Setup...
                    Filter Sets (Firewalls)...
                    IP Address Serving...

                    Date and Time...

                    Console Configuration...

                    SNMP (Simple Network Management Protocol)...

                    Security...

                    Upgrade Feature Set...


                    Logging...

Return/Enter to configure Networking Protocols (such as TCP/IP).
Use this screen if you want options beyond Easy Setup.
```

IP setup

These screens allow you to configure your network's use of IP.

- Details are given in Chapter 9, "IP Setup and Network Address Translation."

Filter sets (firewalls)

These screens allow you to configure security on your network by means of filter sets and a basic firewall.

- Details are given in Chapter 13, "Security."

IP address serving

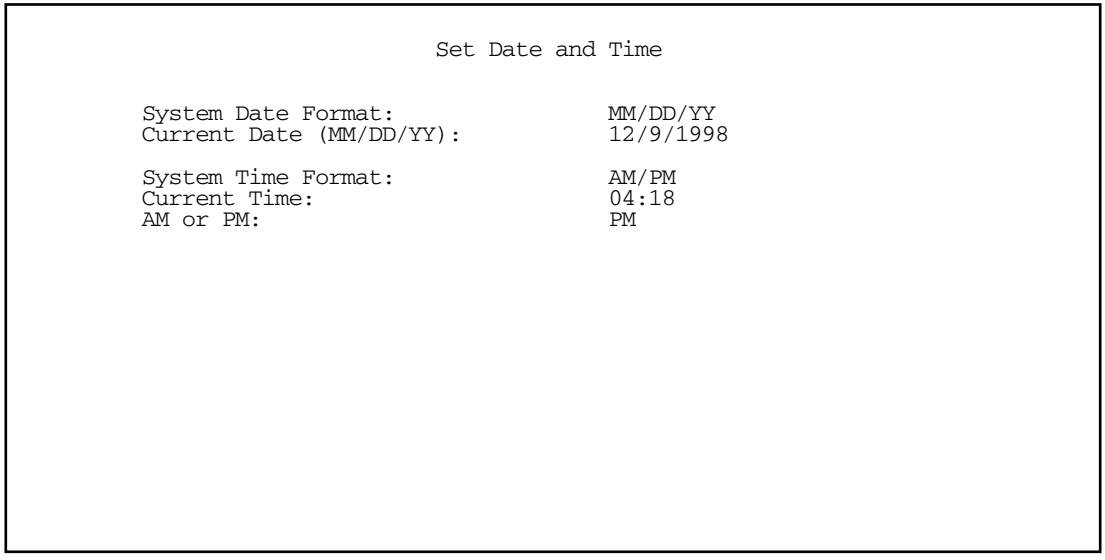
These screens allow you to configure IP address serving on your network by means of DHCP, WANIP, and BootP.

- Details are given in "IP address serving" on page 9-66.

Date and time

You can set the system's date and time in the Set Date and Time screen.

Select **Date and Time** in the System Configuration screen and press Return. The Set Date and Time screen appears.



Follow these steps to set the system's date and time:

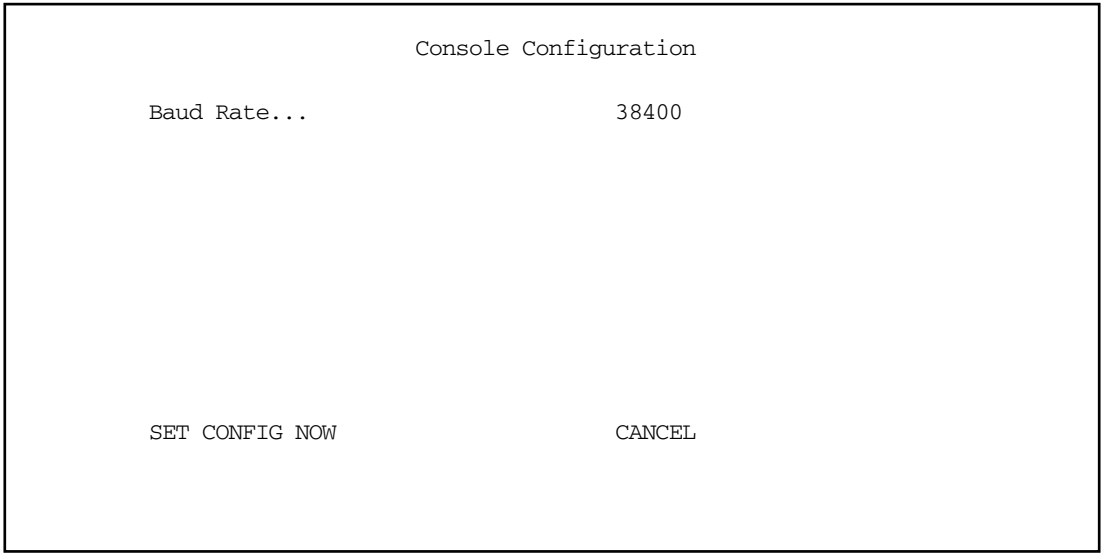
1. Select **Current Date** and enter the date in the appropriate format. Use one- or two-digit numbers for the month and day, and the last two digits of the current year. The date's numbers must be separated by forward slashes (/).
2. Select **Current Time** and enter the time in the format HH:MM, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.

3. Select **AM or PM** and choose **AM** or **PM**.

Console configuration

You can change the default terminal communications parameters to suit your requirements.

To go to the Console Configuration screen, select **Console Configuration** in the System Configuration screen.



Follow these steps to change a parameter's value:

1. Select the parameter you want to change.
2. Select a new value for the parameter. Return to step 1 if you want to configure another parameter.
3. Select **SET CONFIG NOW** to save the new parameter settings. Select **CANCEL** to leave the parameters unchanged and exit the Console Configuration screen.

SNMP (Simple Network Management Protocol)

These screens allow you to monitor and configure your network by means of a standard Simple Network Management Protocol (SNMP) agent.

- Details are given in "SNMP" on page 12-118.

Security

These screens allow you to add users and define passwords on your network.

- Details are given in Chapter 13, "Security."

Upgrade feature set

You can upgrade your Netopia R910 by adding new feature sets through the Upgrade Feature Set utility.

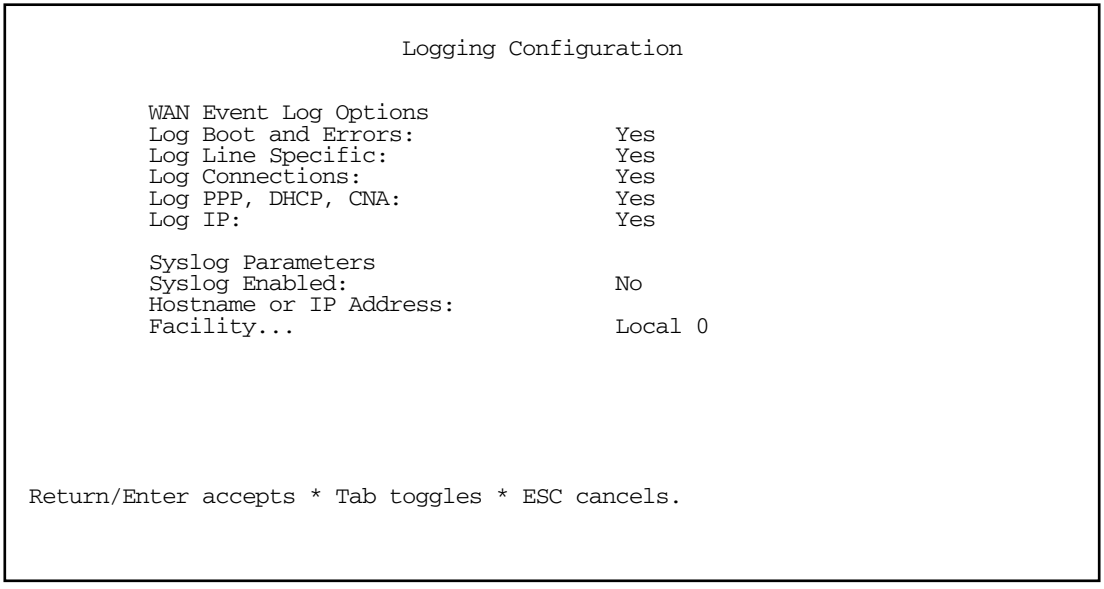
See the release notes that came with your router or feature set upgrade, or visit the Netopia Web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Netopia R910.

Logging

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the router's WAN Event History. See "WAN Event History" on page 12-113.The Syslog client (for the PC only) is supplied as a .ZIP file on the Netopia CustomerCare CD.

Select **Logging** from the System Configuration menu.

The Logging Configuration screen appears.



By default, all events are logged in the event history.

- By toggling each event descriptor either **Yes** or **No**, you can determine which ones are logged and which are ignored.
- You can enable or disable the syslog client dynamically. When enabled, it will report any appropriate and previously unreported events.
- You can specify the syslog server's address either in dotted decimal format or as a DNS name up to 63 characters.
- You can specify the UNIX syslog Facility to use by selecting the **Facility** pop-up.

Installing the Syslog client

The Goodies folder on the Netopia CD contains a Syslog client daemon program that can be configured to report the WAN events you specified in the Logging Configuration screen.

To install the Syslog client daemon, exit from the graphical Netopia CD program and locate the CD directory structure through your Windows desktop, or through Windows Explorer. Go to the Goodies directory on the CD and locate the Sds15000.exe program. This is the Syslog daemon installer. Run the Sds15000.exe program and follow the on screen instructions for enabling the Windows Syslog daemon.

The following screen shows a sample syslog dump of WAN events:

```
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: PPP PAP failure
Nov  5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: Manual disconnect
Nov  5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: No answer
Nov  5 10:14:06 tsnext.netopia.com --Device restarted----------------------------------------
Nov  5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
Nov  5 10:14:06 tsnext.netopia.com   Requested Connect to our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   ASYNC: Modem carrier detected (more) Modem reports: 26400
V34
Nov  5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 activated at 115 Kbps
Nov  5 10:14:06 tsnext.netopia.com   Connect Confirmed to our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   PPP: Channel 1 up, Answer Profile name: Default Profile
Nov  5 10:14:06 tsnext.netopia.com    PPP: NCP up, session 1, Channel 1 Final (fallback)
negotiated auth: Local PAP , Remote NONE
Nov  5 10:14:06 tsnext.netopia.com   PPP: PAP  we accepted remote, Channel 1 Remote name: guest
Nov  5 10:14:06 tsnext.netopia.com    PPP: MP negotiated, session 1 Remote EDO: 06 03
0000C5700624 0
Nov  5 10:14:06 tsnext.netopia.com   PPP: CCP negotiated, session 1, type: Ascend LZS Local
mode: 1, Remote mode: 1
Nov  5 10:14:06 tsnext.netopia.com   PPP: BACP negotiated, session 1 Local MN: FFFFFFFF, Remote
MN: 00000001
Nov  5 10:14:06 tsnext.netopia.com   PPP: IPCP negotiated, session 1, rem: 192.168.10.100 local:
192.168.1.1
Nov  5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 deactivated
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Ind. from DN: 5108645534, Cause: 0
Nov  5 10:14:06 tsnext.netopia.com   Issued Clear Response to DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: Remote clearing
Nov  5 10:14:06 tsnext.netopia.com   PPP: IPCP down, session 1
Nov  5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
```

Chapter 9

IP Setup and Network Address Translation

The Netopia R910 uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the Router to route IP traffic. You also learn how to configure the router to serve IP addresses to hosts on your local network.

The Netopia R910 features IP address serving and Network Address Translation. For a detailed discussion of Network Address Translation, see Appendix C, "Understanding Netopia NAT Behavior" This chapter describes how to use the Network Address Translation feature.

This section covers the following topics:

Network Address Translation allows communication between the LAN connected to the Netopia R910 and the Internet using a single IP address instead of a routed account with separate IP addresses for each computer on the network.

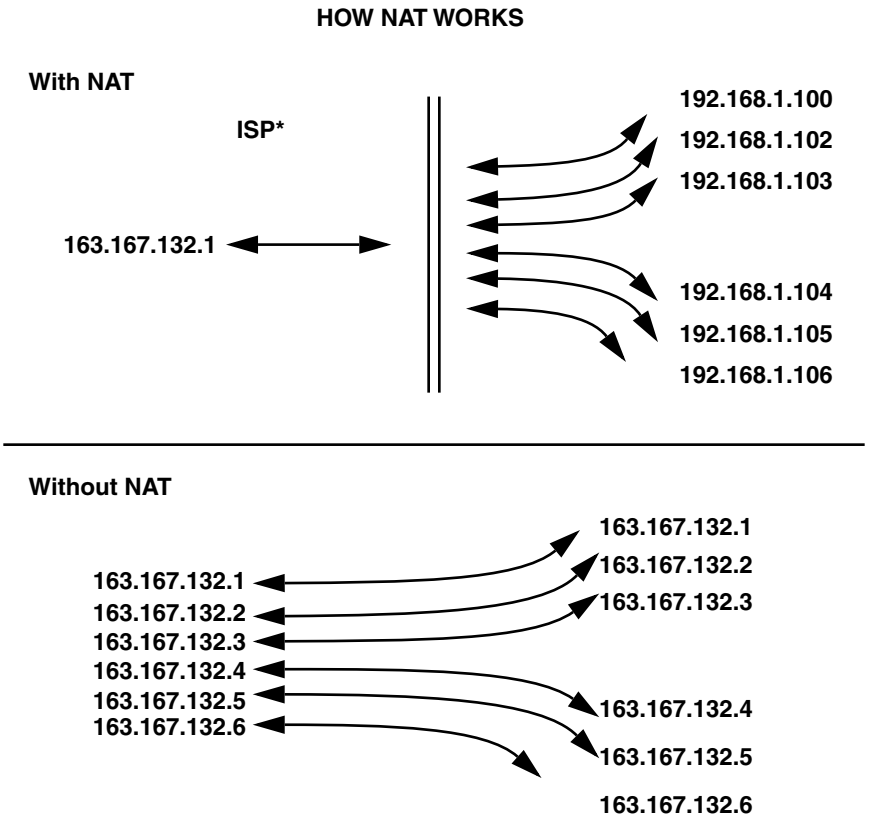
Network Address Translation also provides increased security by hiding the local IP addresses of the LAN connected to the Netopia R910 from the outside world.

Network Address Translation features

Network Address Translation (NAT) offers users the following features:

- The single proxy address is acquired at connection time from the answering side. The address can be assigned by the remote router from either a dynamic pool of addresses or a fixed, static address.
- Static NAT Security is simpler and more reliable because only one IP address needs a firewall, and because the internal network structure is not visible from the Internet.

Network Address Translation works by remapping the source IP address of traffic from the LAN to a single static or dynamically assigned IP address shown to the remote side of the router.



When NAT is enabled, the Netopia R910 can use either a statically assigned IP address or one dynamically assigned each time the router connects to the ISP. While a dynamically assigned IP address offers the ISP more flexibility, it does have an important limitation: the router requires a static IP address to support Web, FTP, or other services available to the WAN. To support these services with NAT enabled, a service can be associated with only one machine on the LAN.

When connected to the Internet or some other large network using Network Address Translation, the individual machines on your LAN are not directly accessible from the WAN. NAT provides an inherently secure method of connection to the outside world.

Using Network Address Translation

The following procedure describes how to use Network Address Translation.

1. Pick a network number for your local network (referred to as the internal network). This can be any IP address range you want. The Netopia R910 Router has a default IP address of 192.168.1.1. You may choose to change this address to match a pre-existing addressing scheme. For this example, we will use 10.0.0.0.

   Note: The outside world (the external network) will not see this network number.

2. Using the internal network number, assign addresses to the local nodes on your LAN. For example, you could assign

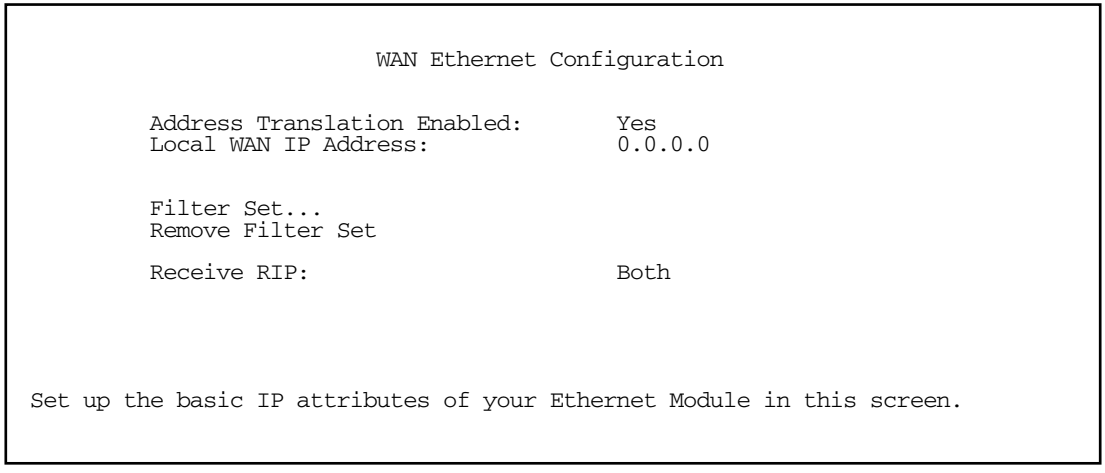
   - 10.0.0.1 to your Netopia R910
   - 10.0.0.2 to a node running as a World Wide Web server
   - 10.0.0.3 to an FTP server
   - 10.0.0.4 to a Windows NT PC
   - 10.0.0.5 to a Windows 95 PC

   Note: See "Associating port numbers with nodes" on page 9-55.

3. By default, Network Address Translation is enabled in the Netopia R910. If you disabled it and now want to reenable it:

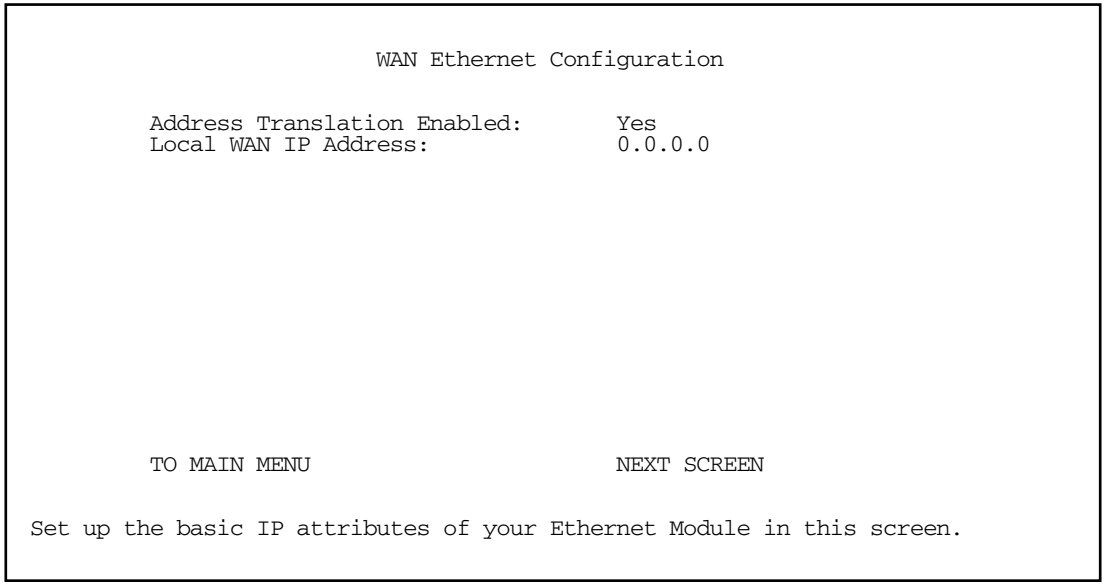
   From the WAN Configuration menu in the Main Menu screen, select **WAN (Wide Area Network) Setup**.

   The WAN Ethernet Configuration screen appears.



   Toggle **Address Translation Enabled** to **Yes** or **No** (Yes to enable NAT) and press Return.

Or, from the Main Menu, select **Easy Setup**. The Easy Setup WAN Ethernet Configuration screen appears.



Toggle **Address Translation Enabled** to **Yes** or **No** (Yes to enable NAT) and press Return.

For more information see Appendix B, "Understanding IP Addressing" and Appendix C, "Understanding Netopia NAT Behavior"

4. If your ISP uses numbered (interface-based) routing, select **Local WAN IP Address** and enter the local WAN address your ISP gave you. Then select **Local WAN IP Mask** and enter the WAN subnet mask of the remote site you will connect to.

   The default address is 0.0.0.0, which allows for dynamic addressing, meaning that your ISP assigns an address via DHCP each time you connect. However, if you want to use static addressing, enter a specific address.

Associating port numbers with nodes

When an IP client such as a Netscape Navigator or Microsoft Internet Explorer, wants to establish a session with an IP server such as a Web server, the client machine must know the IP address to use and the TCP service port where the traffic is to be directed.

For example, a Web browser locates a Web server by using a combination of the IP address and TCP port that the client machine has set up. Just as an IP address specifies a particular computer on a network, ports are addresses that specify a particular service in a computer. There are many universally agreed-upon ports assigned to various services. For example:

- Web servers typically use port number 80
- All FTP servers use port number 21
- Telnet uses port number 23
- SNMP uses port number 161

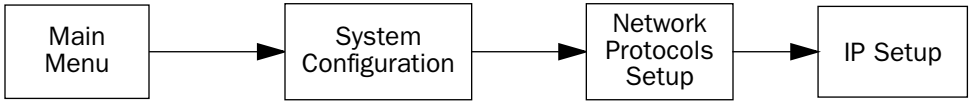
To help direct incoming IP traffic to the appropriate server, the Netopia R910 lets you associate these and other port numbers with distinct IP addresses on your internal LAN using exported services. See "IP setup" on page 9-56 for details.

Network Address Translation guideline

Observe the following guideline when using Network Address Translation.

The router can export only one local IP address per UDP/TCP port, so you can have just one machine available for a given service, such as one FTP server. However, some services, such as Web servers (www-http servers), allow you to change the UDP/TCP port on both the server and client. With two different UDP/TCP ports exported, you can have Web servers on two different IP hosts.

IP setup



The IP Setup options screen is where you configure the Ethernet side of the Netopia R910. The information you enter here controls how the router routes IP traffic.

Consult your network administrator or Internet service provider to obtain the IP setup information (such as the Ethernet IP address, Ethernet subnet mask, default IP gateway and Primary Domain Name Server IP address) you will need before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia R910 is reset.

To go to the IP Setup options screen, from the Main Menu, select **System Configuration** then **Network Protocols Setup**, and then **IP Setup**.

The IP Setup screen appears.

```
                                IP Setup


          Ethernet IP Address:                192.128.117.162
          Ethernet Subnet Mask:               255.255.255.0
          Define Additional Subnets...

          Default IP Gateway:                 192.128.117.163

          Primary Domain Name Server:         0.0.0.0
          Secondary Domain Name Server:       0.0.0.0
          Domain Name:

          Receive RIP:                        Both
          Transmit RIP:                       v2 (multicast)
          Static Routes...

          Address Serving Setup...
          Exported Services...
          Filter Sets...


Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Set up the basic IP attributes of your Netopia in this screen.
```

Follow these steps to configure IP Setup for your Netopia R910:

- Select **Ethernet IP Address** and enter the IP address for the Netopia R910's Ethernet port.
- Select **Ethernet Subnet Mask** and enter the subnet mask for the Ethernet IP address that you entered in the last step.
- If you desire multiple subnets select **Define Additional Subnets**. If you select this item you will be taken to the IP Subnets screen. This screen allows you to define IP addresses and masks for additional subnets. See "IP subnets" on page 9-60 for details.

The Netopia R910 Router supports multiple IP subnets on the Ethernet interface. You may want to configure multiple IP subnets to service more hosts that are possible with your primary subnet. It is not always possible to obtain a larger subnet from your ISP. For example, if you already have a full Class C subnet, your only option is multiple Class C subnets, since it is virtually impossible to justify a Class A or Class B assignment. This assumes that you are not using NAT.

If you are using NAT, you can use the reserved Class A or Class B subnet.

- Select **Default IP Gateway** and enter the IP address for a default gateway. This can be the address of any major router accessible to the Netopia R910.

  A default gateway should be able to successfully route packets when the Netopia R910 cannot recognize the intended recipient's IP address. A typical example of a default gateway is the ISP's router.

- Select **Primary Domain Name Server** and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, robin.hood.com) to the IP addresses actually used by IP routers (for example, 163.7.8.202).

- If a secondary DNS server is available, select **Secondary Domain Name Server** and enter its IP address. The secondary DNS server is used by the Netopia R910 when the primary DNS server is inaccessible. Entering a secondary DNS is useful but not necessary.

- Select **Domain Name** and enter your network's domain name (for example, netopia.com).

- Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia R910 needs to recognize. If this is the case select **Receive RIP** and select **v1**, **v2**, or **Both** from the popup menu. With Receive RIP set to "v1," the Netopia R910's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to "v2," the Netopia R910 will accept routing information provided by RIP packets from other routers that use different subnet masks. Set to "Both," the Netopia R910 will accept information from either RIP v1 or v2 routers.

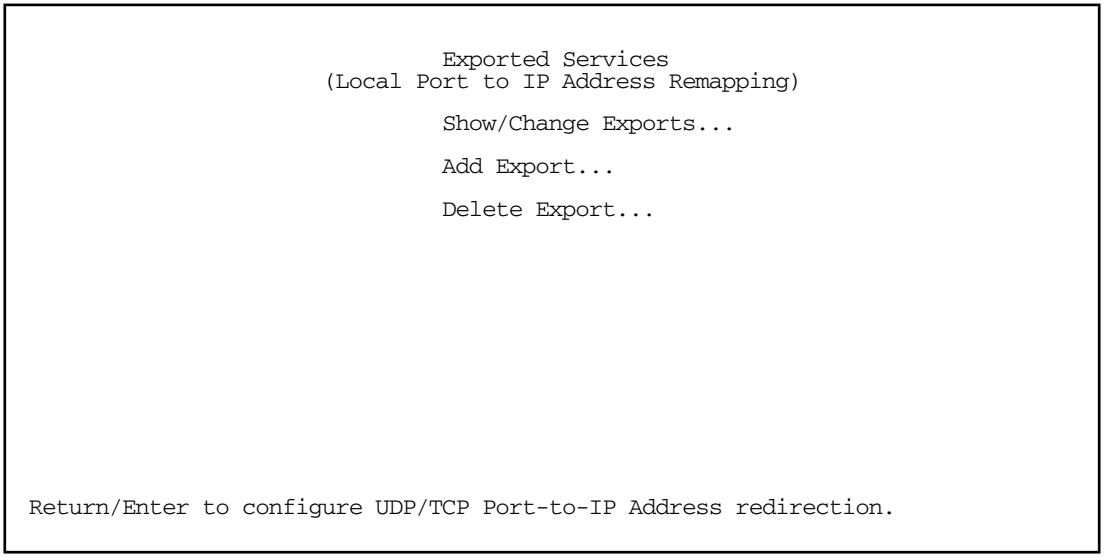
- If you want the Netopia R910 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia R910 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia R910 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia R910 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

- Select **Static Routes** to manually configure IP routes. See the section "Static routes," below.

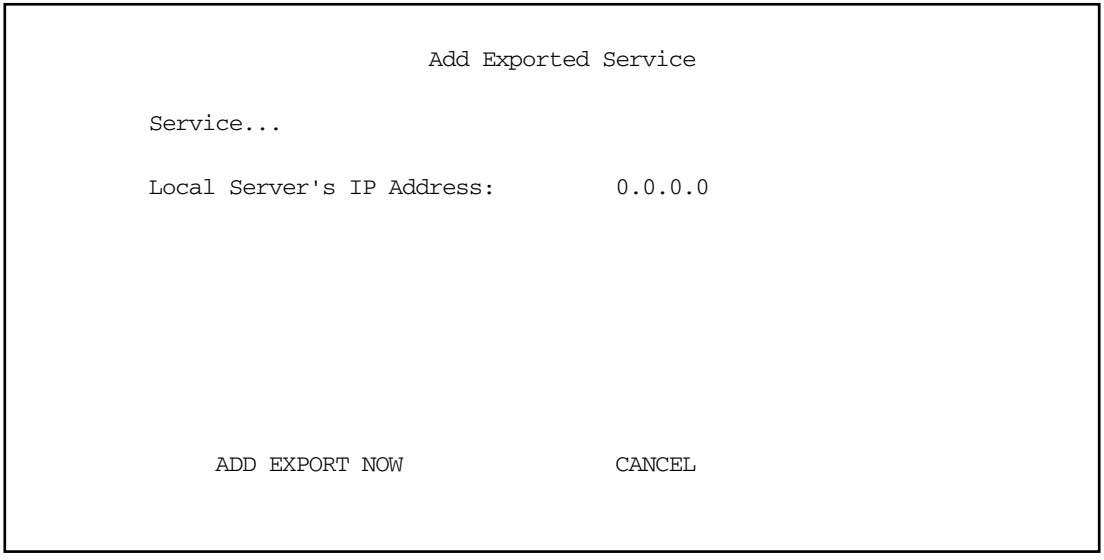
- If you select **Address Serving Setup** you will be taken to the IP Address Serving screen (see "IP address serving" on page 9-66. Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia R910, and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

- Select **Exported Services.** The Exported Services screen appears with three options: Show/Change

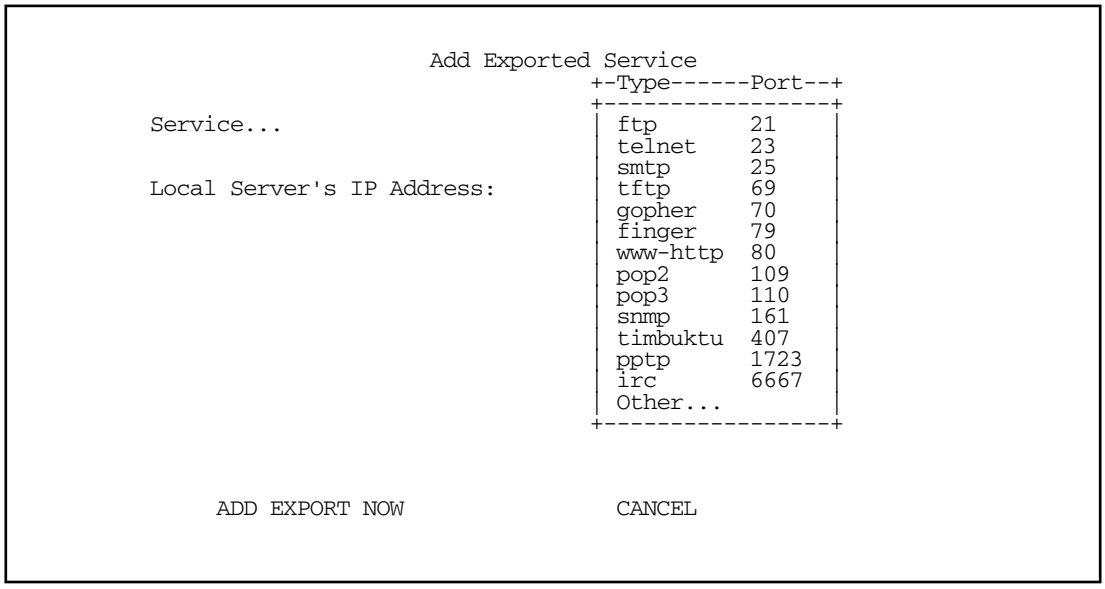
Exports, Add Export, and Delete Export.



- Select **Add Export**. The Add Exported Service screen appears.



- Select **Service**. A pop-up menu of services and ports appears.



5. Select any of the services/ports and press Return to associate it with the address of a server on your local area network. For example, if we select **www-http 80**, press Return, and type **10.0.0.2**, the Netopia R910 redirects any incoming traffic destined for a Web server to address 10.0.0.2.

   Some services such as Timbuktu require the export of multiple TCP ports. When you associate Timbuktu with a local server (or Timbuktu host) all of the major Timbuktu services are exported, i.e., Observe, Control, Send, and Exchange.

Note: If the TCP port of a service you want to use is not listed, you can add it by selecting **Other...** on the pop-up menu.

Press Escape when you are finished configuring exported services. You are returned to the IP Setup screen.

```
                              IP Setup


Ethernet IP Address:                  192.128.117.162
Ethernet Subnet Mask:                 255.255.255.0
Define Additional Subnets...

Default IP Gateway:                   192.128.117.163

Primary Domain Name Server:           0.0.0.0
Secondary Domain Name Server:         0.0.0.0
Domain Name:

Receive RIP:                          Both
Transmit RIP:                         v2 (multicast)
Static Routes...

Address Serving Setup...
Exported Services...
Filter Sets...
```

- If you select **Filter Sets** you will be taken directly to the screen for configuring IP packet filters. For information see "About filters and filter sets," beginning on page 13-126.

IP subnets

The IP Subnets screen allows you to configure up to eight Ethernet IP subnets on unlimited-user models, one "primary" subnet and up to seven secondary subnets, by entering IP address/subnet mask pairs:

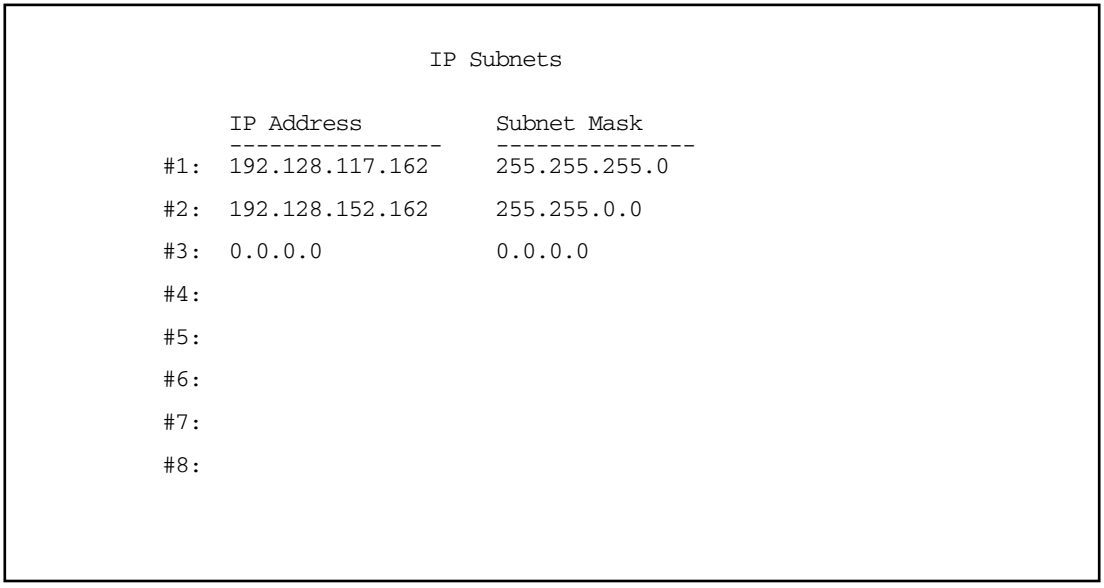
```
                          IP Subnets

      IP Address          Subnet Mask
      ---------------     --------------
#1:   192.128.117.162     255.255.255.0

#2:   0.0.0.0             0.0.0.0

#3:

#4:

#5:

#6:

#7:

#8:
```

Note: You need not use this screen if you have only a single Ethernet IP subnet. In that case, you can continue to enter or edit the IP address and subnet mask for the single subnet on the IP Setup screen.

This screen displays up to eight rows of two editable columns, preceded by a row number between one and eight. If you have eight subnets configured, there will be eight rows on this screen. Otherwise, there will be one more row than the number of configured subnets. The last row will have the value 0.0.0.0 in both the IP address and subnet mask fields to indicate that you can edit the values in this row to configure an additional subnet. All eight row labels are always visible, regardless of the number of subnets configured.

- To add an IP subnet, enter the Netopia R910's IP address on the subnet in the **IP Address** field in a particular row and the subnet mask for the subnet in the **Subnet Mask** field in that row.

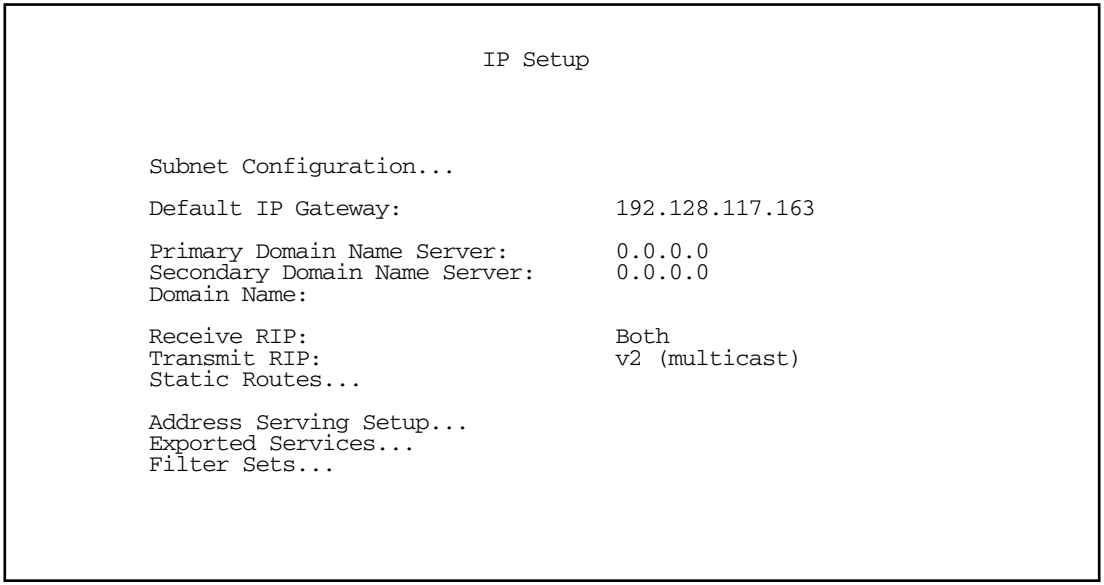
  For example:



- To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and pressing Return or Enter to commit the change. When a configured subnet is deleted, the values in subsequent rows adjust up to fill the vacant fields.

Note that the subnets configured on this screen are tied to the address serving pools configured on the IP Address Pools screen, and that changes on this screen may affect the IP Address Pools screen. In particular, deleting a subnet configured on this screen will delete the corresponding address serving pool, if any, on the IP Address Pools screen.

If you have configured multiple Ethernet IP subnets, the IP Setup screen changes slightly:



The IP address and Subnet mask items are hidden, and the "Define Additional Subnets..." item becomes "Subnet Configuration...". If you select **Subnet Configuration**, you will return to the IP Subnets screen that allows you to define IP addresses and masks for additional Ethernet IP subnets.

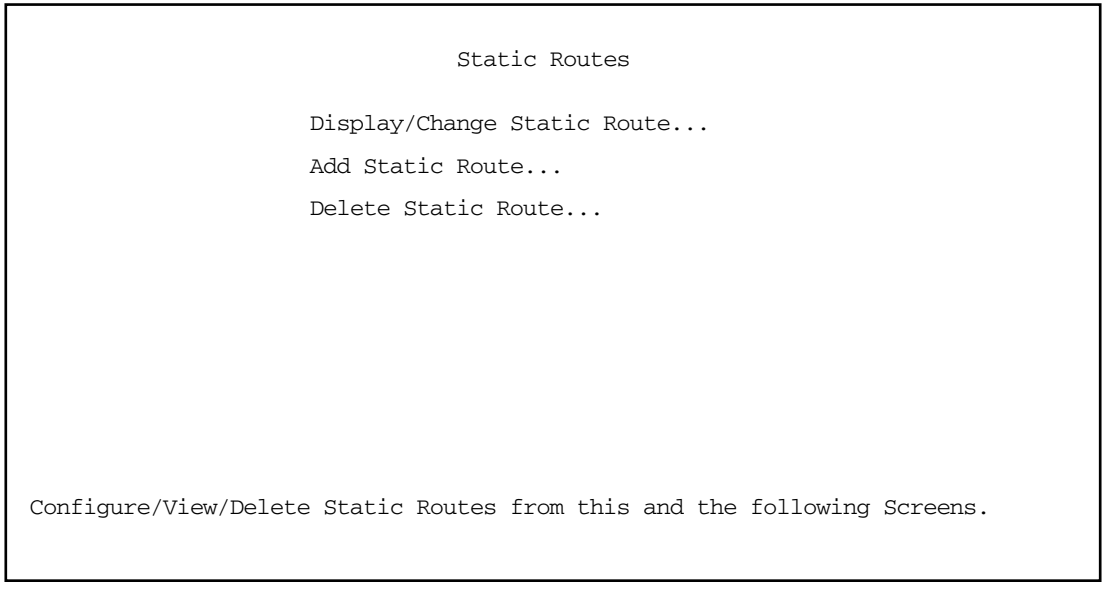
Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Netopia R910 how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Netopia R910 (see "IP routing table" on page 12-115).

Static routes are helpful in situations where a route to a network must be used and other means of finding the route are unavailable. For example, static routes are useful when you cannot rely on RIP.

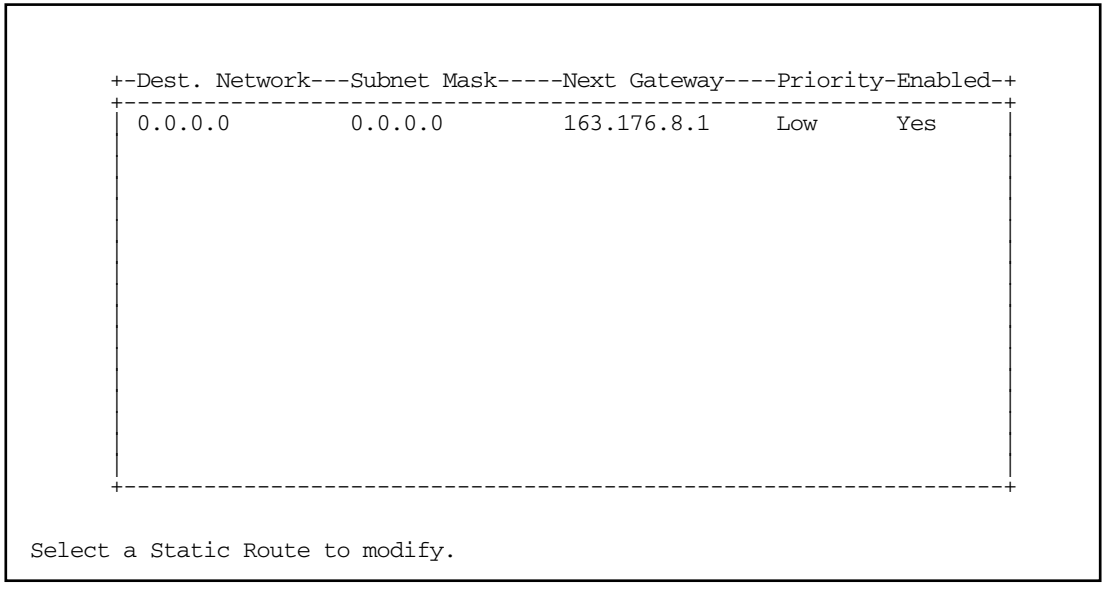
To go to the Static Routes screen, select **Static Routes** in the **IP Setup** screen.

The Static Routes screen will appear.



Viewing static routes

To display a view-only table of static routes, select **Display/Change Static Route**. The table shown below will appear.



The table has the following columns:

Dest. Network: The network IP address of the destination network.

Subnet Mask: The subnet mask associated with the destination network.

Next Gateway: The IP address of the router that will be used to reach the destination network.

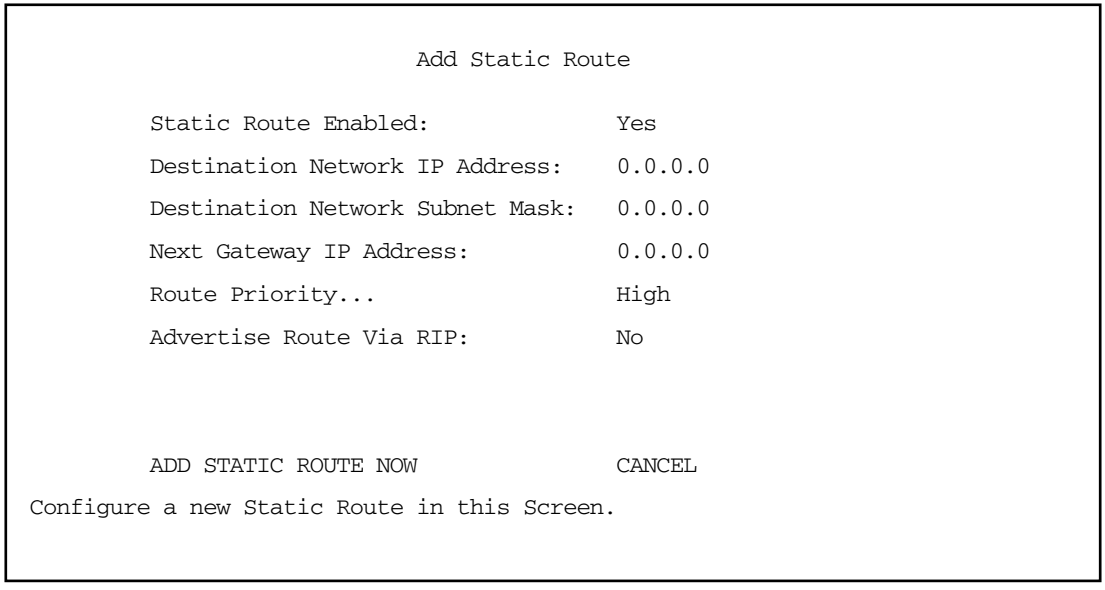
Priority: An indication of whether the Netopia R910 will use the static route when it conflicts with information received from RIP packets.

Enabled: An indication of whether the static route should be installed in the IP routing table.

To return to the Static Routes screen, press Escape.

Adding a static route

To add a new static route, select **Add Static Route** in the Static Routes screen. The Add Static Route screen will appear.



- To install the static route in the IP routing table, select **Static Route Enabled** and toggle it to **Yes**. To remove the static route from the IP routing table, select **Static Route Enabled** and toggle it to **No**.
- Be sure to read the rules on the installation of static routes in the IP routing table. See "Rules of static route installation" on page 9-65.
- Select **Destination Network IP Address** and enter the network IP address of the destination network.
- Select **Destination Network Subnet Mask** and enter the subnet mask used by the destination network.
- Select **Next Gateway IP Address** and enter the IP address for the router that the Netopia R910 will use to reach the destination network. This router does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.
- Select **Route Priority** and choose **High** or **Low**. **High** means that the static route takes precedence over RIP information; **Low** means that the RIP information takes precedence over the static route.
- To make sure that the static route is known only to the Netopia R910, select **Advertise Route Via RIP** and toggle it to **No**. To allow other RIP-capable routers to know about the static route, select **Advertise Route**

Via RIP and toggle it to **Yes**. When Advertise Route Via RIP is toggled to Yes, a new item called RIP Metric appears below Advertise Route Via RIP.

With RIP Metric you set the number of routers, from 1 to 15, between the sending router and the destination router. The maximum number of routers on a packet's route is 15. Setting **RIP Metric** to **1** means that a route can involve 15 routers, while setting it to **15** means a route can only involve one router.

- Select **ADD STATIC ROUTE NOW** to save the new static route, or select **CANCEL** to discard it and return to the Static Routes screen.
- Up to 16 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in system configuration.

Modifying a static route

To modify a static route, in the Static Routes screen select **Display/Change Static Route** to display a table of static routes.

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see "Adding a static route" on page 9-64).

Deleting a static route

To delete a static route, in the Static Routes screen select **Delete Static Route** to display a table of static routes. Select a static route from the table and press Return to delete it. To exit the table without deleting the selected static route, press Escape.

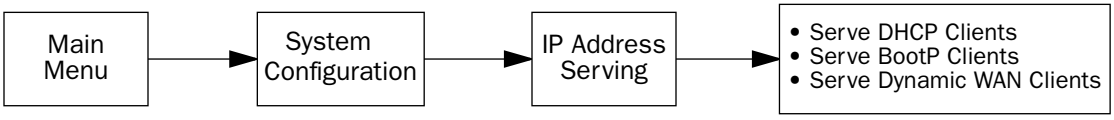
Rules of static route installation

The Netopia R910 applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

- The static route's **Next Gateway IP Address** matches the IP address used by the Netopia R910's Ethernet port.
- The static route's **Next Gateway IP Address** matches an IP address in the range of IP addresses being distributed by MacIP or DHCP.
- The static route's **Next Gateway IP Address** is determined to be unreachable by the Netopia R910.

A static route that is already installed in the IP routing table will be removed if any of the conditions listed above become true for that static route. However, an enabled static route is automatically reinstalled once the conditions listed above are no longer true for that static route.

IP address serving



In addition to being a router, the Netopia R910 is also an IP address server. There are three protocols it can use to distribute IP addresses.

- The first, called **Dynamic Host Configuration Protocol (DHCP)**, is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are "leased" or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.
- The second, called **BootP** (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BootP address assignments are "permanent" since there is no lease renewal mechanism in BootP.
- The third protocol, called **Dynamic WAN**, is part of the PPP/MP suite of wide area protocols used for WAN connections. It allows remote terminal adapters and NAT-enabled routers to be assigned a temporary IP address for the duration of their connection.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia R910 and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

Go to the System Configuration screen. Select **IP Address Serving** and press Return. The IP Address Serving screen will appear.

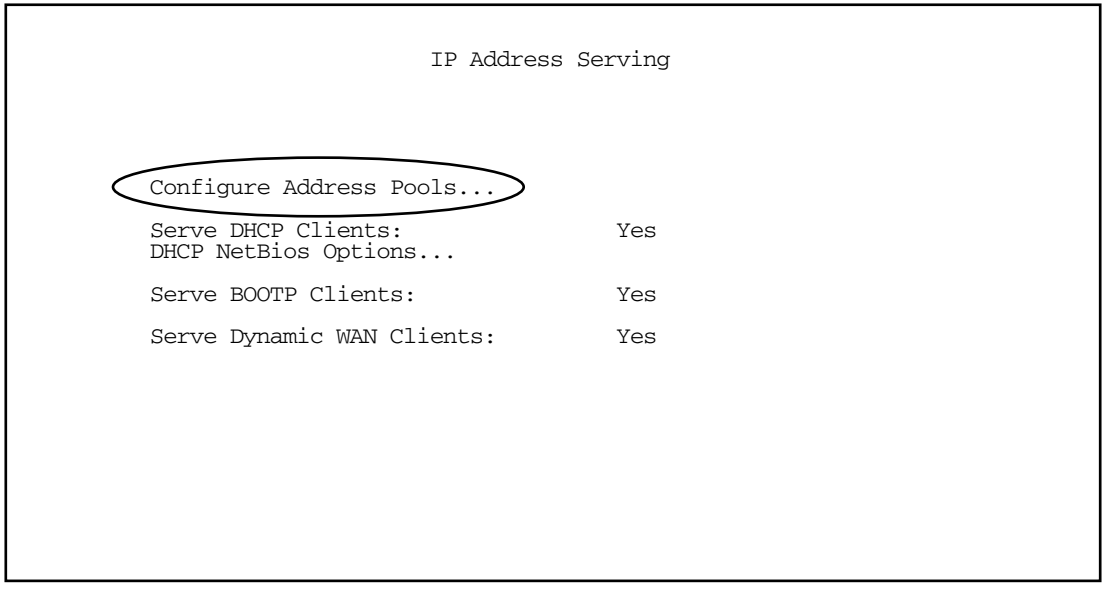
```
                        IP Address Serving

Number of Client IP Addresses:     5
1st Client Address:                176.163.222.10
Client Default Gateway...          176.163.222.1


Serve DHCP Clients:                Yes
DHCP NetBios Options...

Serve BOOTP Clients:               Yes
```

Follow these steps to configure IP Address Serving:

- If you enabled IP Address Serving, DHCP, BootP clients, Dynamic WAN clients, and MacIP/KIP clients (if you have the AppleTalk kit installed) are automatically enabled.
- Select **Number of Client IP Addresses** and enter the total number of contiguous IP addresses that the Netopia R910 will distribute to the client machines on your local area network. 12-user models are limited to twelve IP addresses.
- In the screen example shown above, five Client IP addresses have been allocated.
- Select **1st Client Address** and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may want to first figure out what machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BootP, Dynamic WAN, and/or MacIP.

  Example: Your ISP has given your Netopia R910 the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet (for more information on IP addressing refer to Appendix B, "Understanding IP Addressing"). Your address range will be from **.137-.143**. In this example you would enter **192.168.6.138** as the 1st Client Address, since the router itself must have an IP address.
- To enable DHCP, select **Serve DHCP Clients** and toggle it to **Yes**. DHCP serving is automatic when IP Address Serving is enabled.

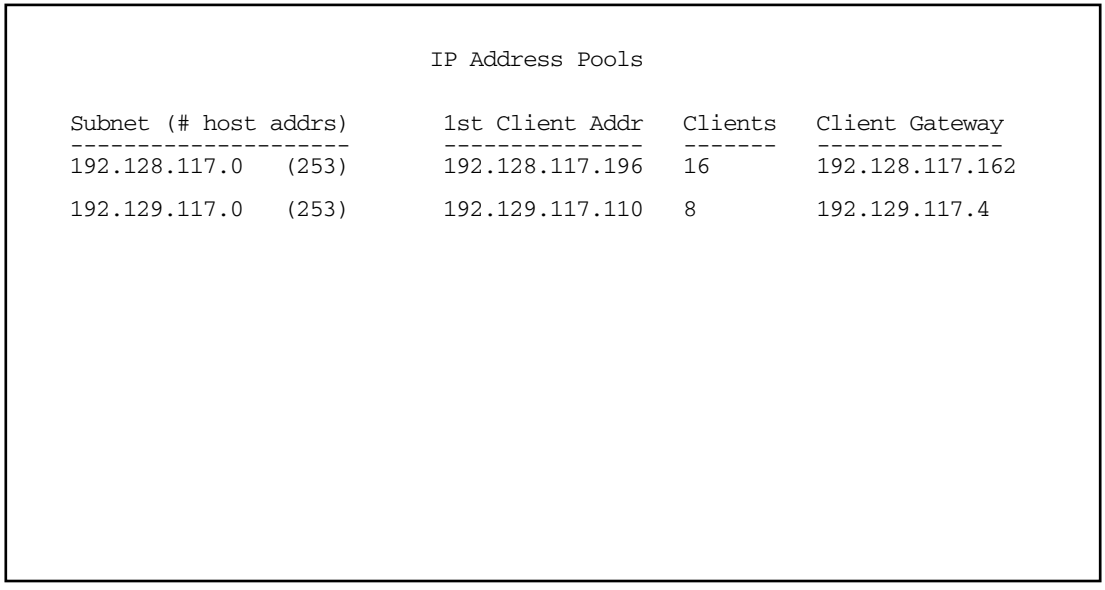
If you have configured multiple Ethernet IP subnets, the appearance of the IP Address Serving screen is altered slightly:



The first three menu items are hidden, and Configure Address Pools appears instead. If you select **Configure Address Pools** you will be taken to the IP Address Pools screen that allows you to configure an address serving pool for each of the configured Ethernet IP subnets. See "IP Address Pools," in the next section.

IP Address Pools

The IP Address Pools screen allows you to configure a separate IP address serving pool for each of up to eight configured Ethernet IP subnets:



This screen consists of between two and eight rows of four columns each. There are exactly as many rows as there are Ethernet IP subnets configured on the IP Subnets screen.

- The Subnet (# host addrs) column is non-selectable and non-editable. It indicates the network address of the Ethernet IP subnet for which an address pool is being configured and the number of host addresses available on the subnet. The network address is equal to the router's IP address on the subnet bitwise-ANDed with the subnet mask. The host address count is equal to the subnet size minus three, since one address is reserved for the network address, one for the subnet broadcast address, and one for the router's interface address on the subnet.

  You can edit the remaining columns in each row.

- The 1st Client Addr and Clients columns allow you to specify the base and extent of the address serving pool for a particular subnet. Entering 0.0.0.0 for the first client address or 0 for the number of clients indicates that no addresses will be served from the corresponding Ethernet IP subnet.

- The Client Gateway column allows you to specify the default gateway address that will be provided to clients served an address from the corresponding pool. The value defaults to the Netopia R910's IP address on the corresponding subnet (or the Netopia R910's default gateway, if that gateway is located on the subnet in question). You can override the value by entering any address that is part of the subnet.

  DHCP, BootP, and dynamic WAN clients may receive an address from any one of the address serving pools configured on this screen.

Numerous factors influence the choice of served address. It is difficult to specify the address that will be served to a particular client in all circumstances. However, when the address server has been configured, and the clients involved have no prior address serving interactions, the Netopia R910 will generally serve the first unused address from the first address pool with an available address. The Netopia R910 starts from the pool on the first row and continues to the pool on the last row of this screen.

Once the address server and/or the clients have participated in address serving transactions, different rules apply:

- When requesting an address, a client will often suggest an address to be assigned, such as the one it was last served. The Netopia R910 will attempt to honor this request if the address is available. The client stores this address in non-volatile storage, for example, on disk, and the specific storage method/location differs depending on the client operating system.
- When requesting an address, a client may provide a client identifier, or, if it does not, the Netopia R910 may construct a pseudo-client identifier for the client. When the client subsequently requests an address, the Netopia R910 will attempt to serve the address previously associated with the client identifier. This is normally the last address served to the client.
- Otherwise, the Netopia will select the least-recently used available address, starting from the first address in the first pool and ending with the last address in the last pool.

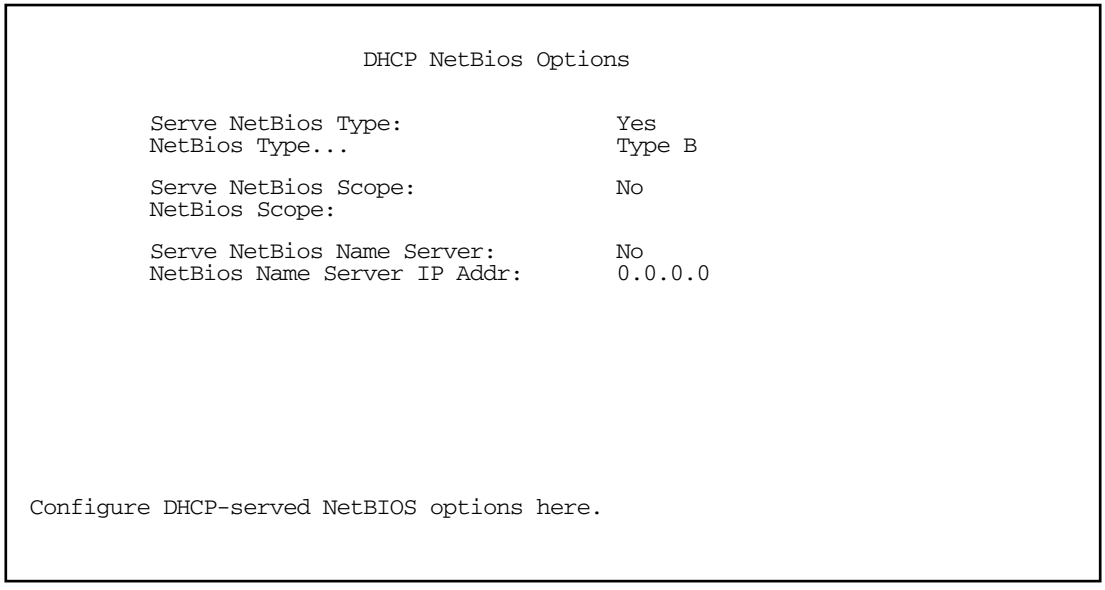
Note that the address serving pools on this screen are tied to the IP subnets configured on the IP Subnets screen. Changes to the IP Subnets screen may affect this one. In particular, deleting a subnet on the IP Subnets screen will delete the corresponding address serving pool, if any, on this screen.

DHCP NetBIOS Options

If your network uses NetBIOS, you can enable the Netopia R910 to use DHCP to distribute NetBIOS information.

NetBIOS stands for Network Basic Input/Output System. It is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. NetBIOS has been adopted as an industry standard. It offers LAN applications a variety of "hooks" to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network. To run an application that works with NetBIOS, a non-IBM network operating system or network interface card must offer a NetBIOS emulator. Many vendors either provide a version of NetBIOS to interface with their hardware or emulate its transport layer communications services in their network products. A NetBIOS emulator is a program provided by NetWare clients that allow workstations to run applications that support IBM's NetBIOS calls.

- Select **DHCP NetBios Options** and press Return. The DHCP NetBIOS Options screen appears.



- To serve DHCP clients with the type of NetBIOS used on your network, select **Serve NetBios Type** and toggle it to **Yes**.

- From the **NetBios Type** pop-up menu, select the type of NetBIOS used on your network.

```
                    DHCP NetBios Options

                                        +---------+
Serve NetBios Type:                     +---------+
NetBios Type...                         | Type B  |
                                        | Type P  |
Serve NetBios Scope:                    | Type M  |
NetBios Scope:                          | Type H  |
                                        +---------+
Serve NetBios Name Server:                No
NetBios Name Server IP Addr:              0.0.0.0
```

- To serve DHCP clients with the NetBIOS scope, select **Serve NetBios Scope** and toggle it to **Yes**.

  Select **NetBios Scope** and enter the scope.

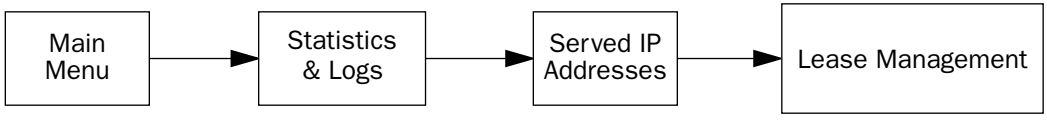
- To serve DHCP clients with the IP address of a NetBIOS name server, select **Serve NetBIOS Name Server** and toggle it to **Yes**.

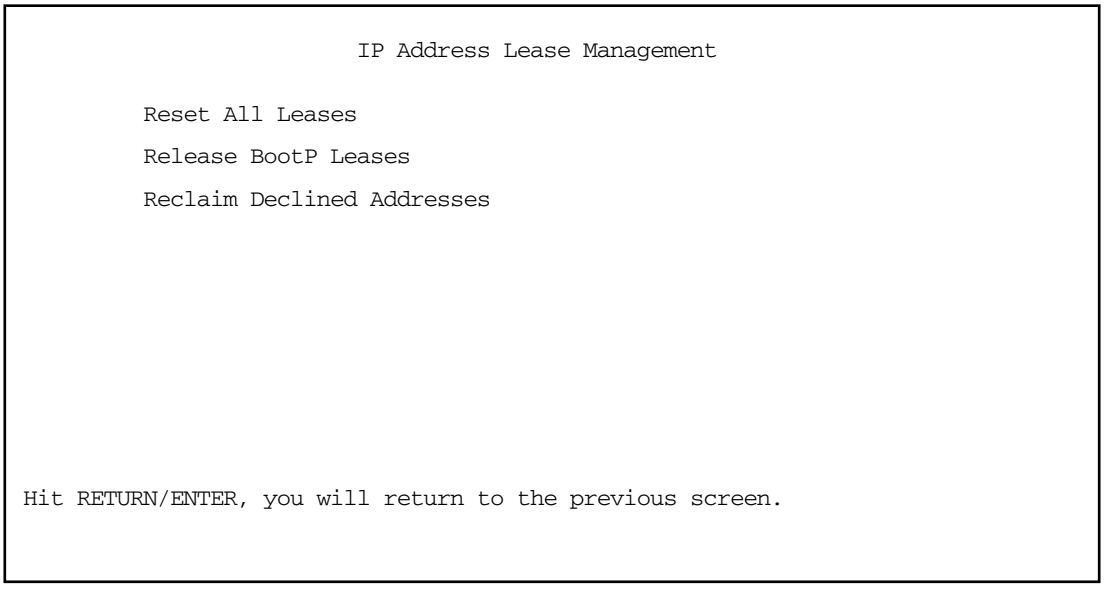
  Select **NetBios Name Server IP Addr** and enter the IP address for the NetBIOS name server.

  You are now finished setting up DHCP NetBIOS Options. To return to the IP Address Serving screen press Escape.

- To enable BootP's address serving capability, select **Serve BOOTP Clients** and toggle to **Yes**.

  Note: Addresses assigned through BootP are permanently allocated from the IP Address Serving pool until you release them. To release these addresses, navigate back to the Main Menu, then Statistics & Logs, Served IP Addresses, and **Lease Management**.





Select **Release BootP Leases** and press Return.

You have finished your IP setup.

Chapter 10

Virtual Private Networks (VPN)

The Netopia R910 Router offers both PPTP and ATMP tunneling support for Virtual Private Networks (VPN).

The following topics are covered in this chapter:

Overview

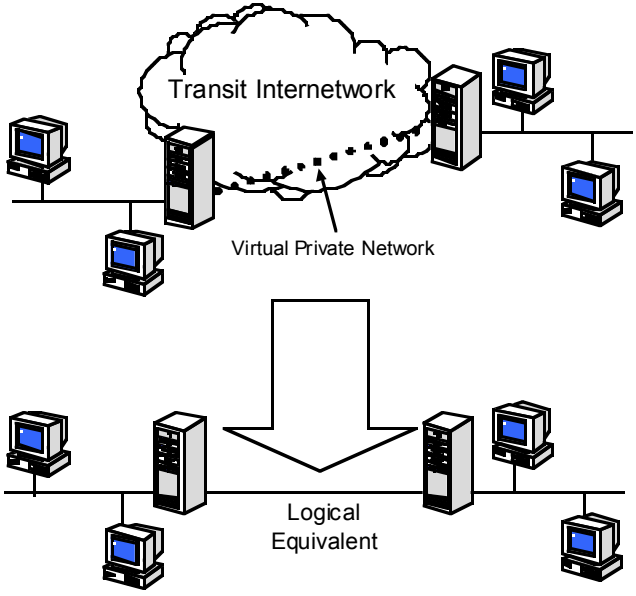
When you make a long distance telephone call from your home to a relative far away, you are creating a private network. You can hold a conversation and exchange information about the happenings on opposite sides of the state, or the continent, that you are mutually interested in. When your next door neighbor picks up the phone to call her daughter at college, at the same time you are talking to your relatives, your calls don't overlap, but each is separate and private. Neither house has a direct wire to the places they call. Both share the same lines on the telephone poles (or underground) on the street.

These calls are *virtual private networks*. *Virtual*, because they appear to be direct connections between the calling and answering parties, even though they travel over the public wires and switches of the phone company; *private*, because neither pair of calling and answering parties interacts with the other; and *networks*, because they exchange information.

Computers can do the same thing; it's called Virtual Private Networks (VPNs). Equipped with Netopia Routers, a single computer or private network (LAN) can establish a private connection with another computer or private network over the public network (Internet).

The Netopia Router can be used in VPNs either to initiate the connection or to answer it. When used in this way, the routers are said to be *tunnelling* through the public network (Internet). The advantages are that, like your long distance phone call, you don't need a direct line between one computer or LAN and the other, but use the local connections, making it much cheaper; and the information you exchange through your tunnel is private and secure.

Tunneling is a process of creating a private path between a remote user or private network and another private network over some intermediate network, such as the IP-based Internet. A VPN allows remote offices or employees access to your internal business LAN through means of encryption allowing the use of the public Internet to look "virtually" like a private secure network. When two networks communicate with each other through a network based on the Internet Protocol, they are said to be *tunneling* through the IP network.



Unlike the phone company, private and public computer networks can use more than one protocol to carry your information over the wires. Three such protocols are in common use for tunnelling, Point-to-Point Tunnelling Protocol (PPTP), IP Security (IPSec), and Ascend Tunnel Management Protocol (ATMP). The Netopia Router can use any of them.

- Point-to-Point Tunneling Protocol (PPTP) is an extension of Point-to-Point Protocol (PPP) and uses a client and server model. Netopia's PPTP implementation is compatible with Microsoft's and can function as either the client (PAC) or the server (PNS). As a client, a Netopia R-series router can provide all users on a LAN with secure access over the Internet to the resources of another LAN by setting up a tunnel with a Windows NT server running Remote Access Services (RAS) or with another Netopia Router. As a server, a Netopia R-series router can provide remote users a secure connection to the resources of the LAN over a dial-up, cable, DSL, or any other type of Internet access. Because PPTP can create a VPN tunnel using the Dial-Up Networking (DUN) (see "Dial-Up Networking for VPN" on page 10-88) utility built into Windows 95, 98, or NT, no additional client software is required.
- IP Security (IPsec) is a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is widely used to implement Virtual Private Networks. *DES* stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key.
- Ascend Tunnel Management Protocol (ATMP) is the protocol that is implemented in many Ascend routers. ATMP is a simple protocol for connecting nodes and/or networks together over the Internet via a tunnel. ATMP encapsulates IP or other user data without PPP headers within General Routing Encapsulation (GRE) protocol over IP. ATMP is more efficient than PPTP for network-to-network tunnels.

When used to initiate the tunnelled connection, the Netopia Router is called a *PPTP Access Concentrator* (*PAC*, in PPTP language), or a *foreign agent* (in ATMP language). When used to answer the tunnelled connection, the Netopia Router is called a *PPTP Network Server* (*PNS*, in PPTP language) or a *home agent* (in ATMP language).

In either case, the Netopia Router wraps, or encapsulates, information that one end of the tunnel exchanges with the other, in a wrapper called General Routing Encapsulation (GRE), at one end of the tunnel, and unwraps, or decapsulates, it at the other end.

Configuring the Netopia Router for use with any of the three protocols is done through the console-based menu screens. Each type is described in its own section:

- "About PPTP Tunnels" on page 10-76
- "About IPsec Tunnels" on page 10-80
- "About ATMP Tunnels" on page 10-94

Your configuration depends on which protocol you (and the router at the other end of your tunnel) will use, and whether or not you will be using the VPN client software in a standalone remote connection.

Note: You must choose which protocol you will be using, since you cannot both export PPTP and use ATMP, or vice versa, at the same time.

Having both an ATMP tunnel and a PPTP export is not possible because both functions require GRE and the router's PPTP export/server does not distinguish the GRE packets it forwards. Since it processes all of them, ATMP tunneling is impaired. For example, you cannot run an ATMP tunnel between two routers and also have PPTP exported on one side.

Summary

A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing you to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks.

VPNs allow networks to communicate across an IP network. Your local networks (connected to the Netopia Router) can exchange data with remote networks that are also connected to a VPN-capable router.

This feature provides individuals at home, on the road, or in branch offices with a cost-effective and secure way to access resources on remote LANs connected to the Internet with Netopia Routers. The feature is built around two key technologies: PPTP and ATMP.

About PPTP Tunnels

To set up a PPTP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote PPTP partner. You use the same procedure to initiate a PPTP tunnel that terminates at a remote PPTP server or to terminate a tunnel initiated by a remote PPTP client.

PPTP configuration

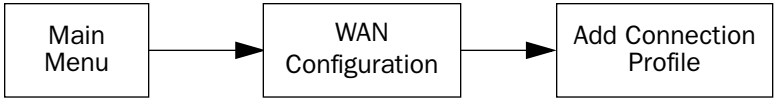
To set up the router as a PPTP Network Server (PNS) capable of answering PPTP tunnel requests you must also configure the VPN Default Answer Profile. See "VPN Default Answer Profile" on page 10-85 for more information.

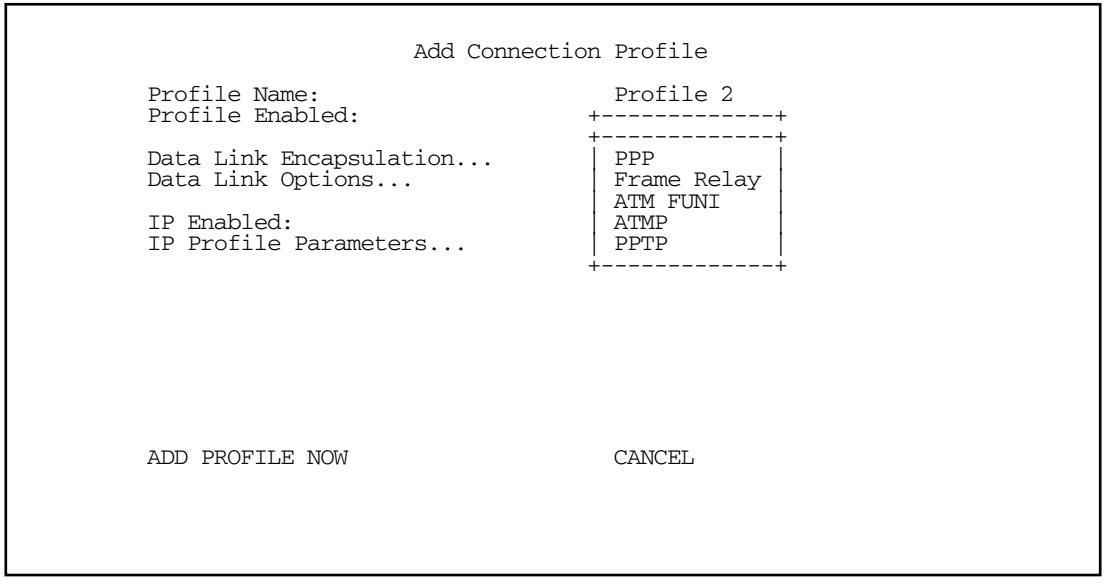
PPTP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, as PPTP is not a native encapsulation. Consequently, the Easy Setup Profile does not offer PPTP datalink encapsulation.

Note: The Netopia R910 Router has access to Connection Profiles for tunnelling purposes. If the PPP dialup kit is not installed, you cannot use PPP as a datalink encapsulation, and you will have access only to ATMP and PPTP. If the kit is installed you also have access to PPP.

Channel 4 (and higher) events, such as connections and disconnections, reported in the WAN Event Histories are VPN tunnel events.

To define a PPTP tunnel, navigate to the Add Connection Profile menu from the Main Menu.





When you define a Connection Profile as using PPTP by selecting PPTP as the datalink encapsulation method, and then select **Data Link Options**, the PPTP Tunnel Options screen appears.

```
                          PPTP Tunnel Options

        PPTP Partner IP Address:          173.167.8.134
        Tunnel Via Gateway:               0.0.0.0

        Data Compression...               None
        Authentication...                 CHAP


        Send Host name:                   tony
        Send Secret:                      *****

        Receive Host name:                kimba
        Receive Secret:                   ******


        Initiate Connections:             Yes
        On Demand:                        Yes

        Idle Timeout (seconds):           300

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
In this Screen you will configure the GRE/PPTP specific connection params.
```

Note: Profiles using PPTP do not offer a Telco Options screen.

- Enter the **PPTP Partner IP Address**. This specifies the address of the other end of the tunnel.

  If you do not specify the PPTP Partner IP Address the gateway cannot initiate tunnels, i.e., act as a PPTP Access Concentrator (PAC) for this profile. It can only accept tunnel requests as a PPTP Network Server (PNS).

- If you specify the PPTP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, the **Tunnel Via Gateway** option becomes visible. You can enter the address by which the gateway partner is reached.

  If you do not specify the PPTP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e., the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.

- You can specify a **Data Compression** algorithm, either None or Standard LZS, for the PPTP connection.

  Note: When the Authentication protocol is MS-CHAP, compression is set to None, and the **Data Compression** option is hidden.

- From the pop-up menu select an **Authentication** protocol for the PPP connection. Options are PAP, CHAP, or MS-CHAP. The default is PAP. The authentication protocol must be the same on both ends of the tunnel.

- When the authentication protocol is MS-CHAP, you can specify a **Data Encryption** algorithm for the PPTP connection. Available options are MPPE and None (the default). For other authentication protocols, this option is hidden. When MPPE is negotiated, the WAN Event History reports that it is negotiated as a CCP (compression) type. This is because the MPPE protocol uses a compression engine, even though it is not itself a compression protocol.

Note: The Netopia R910 Router supports 128-bit ("strong") encryption and MS-CHAP Version 2. Unlike MS-CHAP version 1, which supports one-way authentication, MS-CHAP version 2 supports mutual authentication between connected routers and is incompatible with MS-CHAP version 1 (MS-CHAP-V1). When you choose MS-CHAP as the authentication method for the PPTP tunnel, the Netopia router will start negotiating MS-CHAP-V2. If the router you are connecting to does not support MS-CHAP-V2, it will fall back to MS-CHAP-V1, or, if the router you are connecting to does not support MPPE at all, the PPP session will be dropped.

- You can specify a **Send Host Name** which is used with Send Secret for authenticating with a remote PNS when the profile is used for initiating a tunnel connection.
- You must specify a **Send Secret** (the CHAP term for password), used for authenticating the tunnel when initiating a tunnel connection.
- You can specify a **Receive Host Name** which is used with the Receive Secret for authenticating a remote PPTP client.
- You must specify a **Receive Secret**, used for authenticating the remote PPTP client.
- You can specify that this router will **Initiate Connections** (acting as a PAC) or only answer them (acting as a PNS).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established via the call management screens or may be scheduled using the scheduled connections feature.
- Some networks that use Microsoft Windows NT PPTP Network Servers require additional authentication information, called *Windows NT Domain Name*, when answering PPTP tunnel connection requests. Not all Windows NT installations require this information, since not all such installations use this authentication feature. The **Optional Windows NT Domain Name** is not the same as the Internet domain name, but is the name of a group of servers that share common security policy and user account databases. Your PPTP tunnel partner's administrator will supply this Windows NT Domain Name if it is required.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return.

The IP Profile Parameters screen appears.

```
                          IP Profile Parameters

        Address Translation Enabled:        Yes

        NAT Map List...                     Easy-PAT
        NAT Server List...                  Easy-Servers

        Local WAN IP Address:               0.0.0.0

        Remote IP Address:                  173.167.8.10
        Remote IP Mask:                     255.255.0.0

        Filter Set...
        Remove Filter Set

        Receive RIP:                        Both


Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
```

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a PAC has NAT applied to a Connection Profile set for PPTP data link encapsulation, the PNS and devices behind it, cannot Ping the PAC's tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia Router is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

Encryption Support

Encryption is a method for altering user data into a form that is unusable by anyone other than the intended recipient. The recipient must have the means to decrypt the data to render it usable to them. The encryption process protects the data by making it difficult for any third party to get at the original data.

Netopia PPTP is fully compatible with Microsoft Point-to-Point Encryption (MPPE) data encryption for user data transfer over the PPTP tunnel. Microsoft Windows NT Server provides MPPE encryption capability only when Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is enabled. Netopia complies with this feature to allow MPPE only when MS-CHAP is negotiated. MS-CHAP and MPPE are user-selectable options in the PPTP Tunnel Options screen. If either the client or the server side specifies encryption, then encryption becomes mandatory for both.

Netopia's ATMP implementation supports Data Encryption Standard (DES) data encryption for user data transfer over the ATMP tunnel between two Netopia routers. The encryption option, None or DES, is a selectable option in the ATMP Tunnel Options screen.

MS-CHAP V2 and strong encryption

Notes:

- The Netopia R910 Router supports 128-bit ("strong") encryption. If the router you are connecting to does not support 128-bit encryption, the Netopia router will default to 40-bit encryption.

  US encryption regulations changed mid-February, 2000, making it possible to include this new encryption feature as a standard part of the firmware. This means that, worldwide, the Netopia R910 Router, because it supports VPN, also supports 128-bit encryption for free, when using PPTP tunnels.

  ATMP does not have an option of using 128-bit MPPE. If you are using ATMP between two Netopia routers you can optionally set 56-bit DES encryption.

- Unlike MS-CHAP version 1, which supports one-way authentication, MS-CHAP version 2 supports mutual authentication between connected routers and is incompatible with MS-CHAP version 1 (MS-CHAPv1). When you choose MS-CHAP as the authentication method for a PPTP tunnel, the Netopia router will start negotiating MS-CHAPv2. If the router or VPN adapter client you are connecting to does not support MS-CHAPv2, the Netopia router will fall back to MS-CHAPv1, or, if the router or VPN adapter client you are connecting to does not support MPPE at all, the PPP session will be dropped. This is done automatically and transparently.

About IPsec Tunnels

IPsec stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement VPNs.

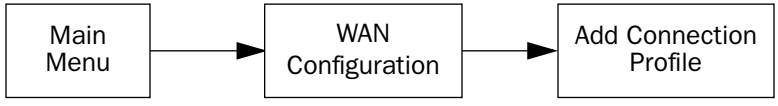
IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. Netopia Routers support the more secure Tunnel mode. The Netopia R910 offers IPsec DES encryption over the VPN tunnel.

DES stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key.

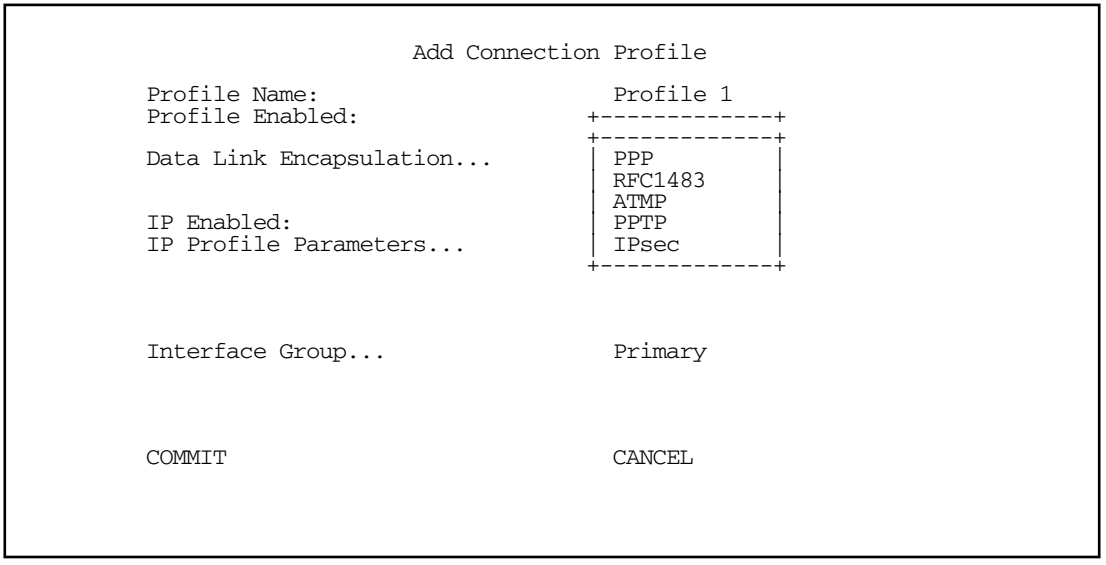
Configuration

IPsec tunnels are defined in the same manner as PPTP tunnels. You configure the Connection Profile as follows.

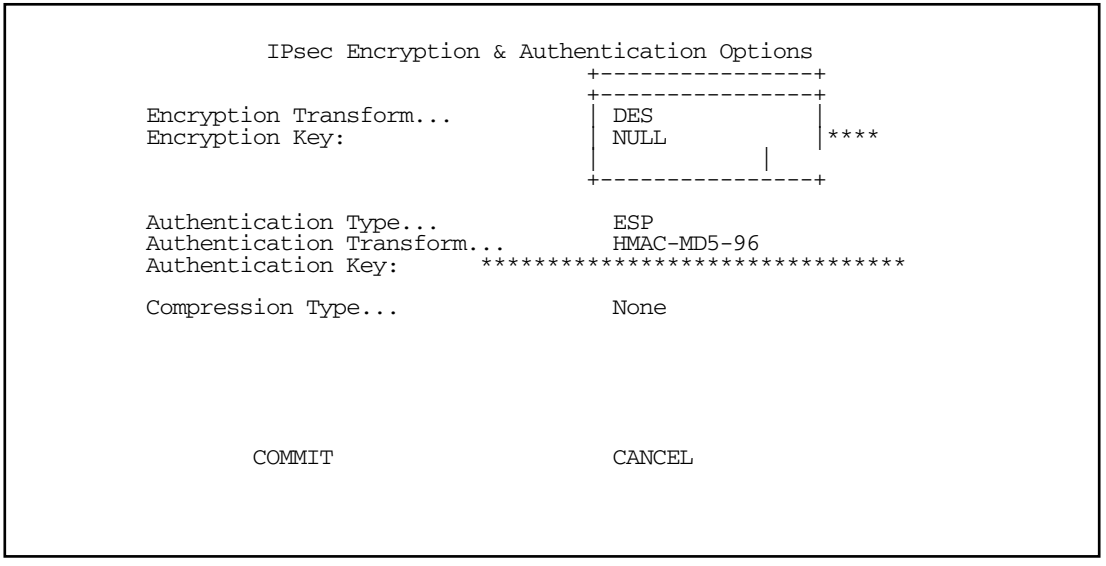
From the Main Menu navigate to WAN Configuration and then Add Connection Profile.



The Add Connection Profile screen appears.

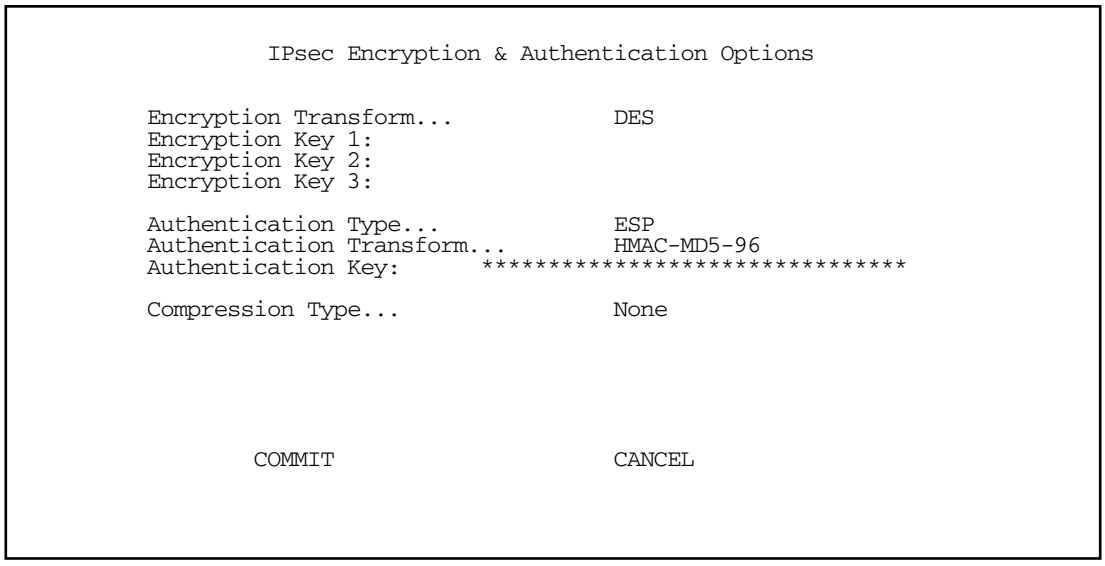


- From the **Data Link Encapsulation** pop-up menu select **IPsec**.
- Then select **Data Link Options**. The IPsec Encryption & Authentication Options screen appears.



The screen offers the following Data Link Options for an IPsec Connection Profile.

- You must specify an **Encryption Transform**. The choices are **DES** or **NULL**. The default is **DES**.



- You must enter an **Encryption Key** or keys if the Encryption Transform is DES. The key must be a hexadecimal entry of eight bytes (16 bytes of input). No key entry appears if the encryption transform is NULL.
- You must specify an **Authentication Type**. The default is **ESP**, and the choices are **ESP**, **None**, or **AH**. **ESP** provides confidentiality over the IP payload and optional authentication of the IP payload and ESP header. **AH** (Authentication Header) provides authentication over the immutable parts of the IP header, AH header and the IP payload. ESP is preferred.
- You must specify an **Authentication Transform** if the Authentication Type is anything other than None. The default is **HMAC-MD5-96**, and the choices are **HMAC-MD5-96** or **HMAC-SHA1-96** for both AH and ESP.
- You must specify an **Authentication Key** if the Authentication Type is anything other than None. The key must be an ASCII string of up to 48 characters for both HMAC-MD5-96 and HMAC-SHA1-96.

  Key: The key is a hexadecimal entry of 16 bytes (32 characters of input) for MD5 and 20 bytes (40 characters of input) for SHA1. It is not possible to view the Encryption Keys or Authentication Key once they have been set.
- You can specify a **Compression Type**. The default is **None**.
- Press **COMMIT** to return to the Add Connection Profile screen.

Note: The Connection Profile is copied to a temporary buffer while it is being modified. Only when the COMMIT button is selected will the profile be updated and the changes applied. This is true of all profiles regardless of encapsulation type.

- Select **IP Profile Parameters**.

IP Profile Parameters

The following IP Profile Options screen is displayed for an IPsec Connection Profile.

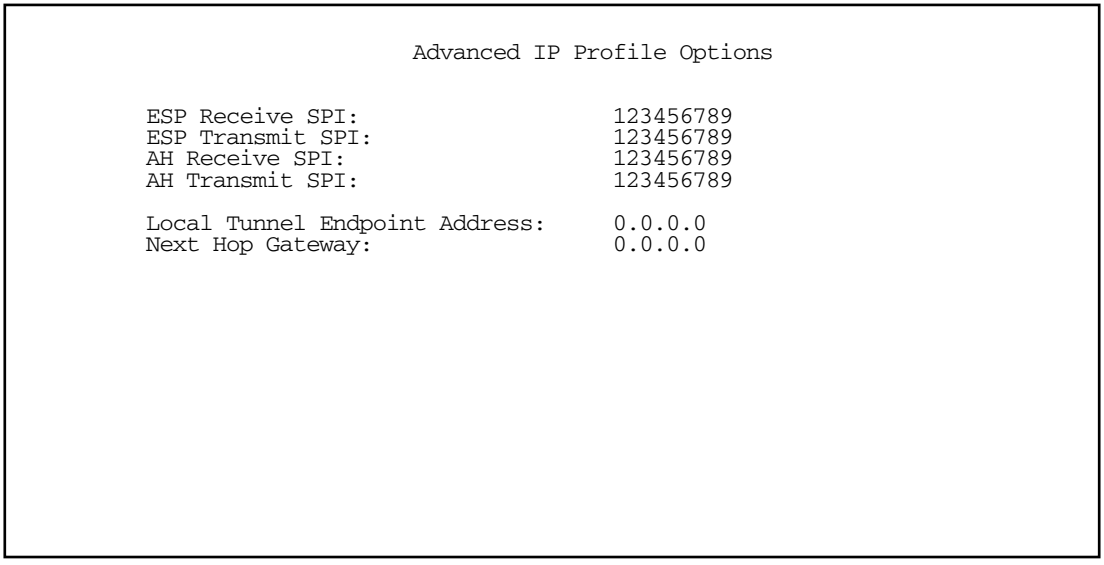
```
                        IP Profile Options

SPI (Security Parameters Index):    123456789

Remote Tunnel Endpoint Address:     0.0.0.0
Remote Members Network:             0.0.0.0
Remote Members Mask:                0.0.0.0

Address Translation Enabled:        Yes
NAT Map List...                     Easy-PAT List
NAT Server List...                  Easy-Servers
PAT IP Address:                     1.1.1.1

Filter Set...                       <<None>>
Remove Filter Set

Advanced IP Profile Options...


        COMMIT                      CANCEL
```

- You must specify an **SPI (Security Parameters Index)**, which is the ESP receive side SPI and the default SPI for ESP transmit, AH receive, and AH transmit. It must be unique relative to any other configuration profile "ESP Receive SPIs." (See "Advanced IP Profile Options" on page 10-84.)
- You must specify a **Remote Tunnel Endpoint Address**. Specify the IP address of your tunnel partner, the endpoint of the tunnel. The Remote Tunnel Endpoint Address may be 0.0.0.0, which implies that the IPsec tunnel will not be established until packets are received on the SPI specified. At that time the tunnel will be bound to the Remote Tunnel Endpoint until traffic from the remote gateway ceases for a timeout period.
- You must specify a **Remote Members Network** address. This specifies the subnet of the remote IPsec tunnel and will be used with the Remote Members Mask to determine and set the route.
- You must specify a **Remote Members Mask**. This is the subnet mask of the remote subnet to which the IPsec tunnel will route.
- You can specify **Address Translation Enabled**. For more information see Chapter 9, "IP Setup and Network Address Translation." If Address Translation Enabled is set to **Yes**, you can specify the following three fields:
  - **NAT Map List**
  - **NAT Server List**
  - **PAT IP Address**
    (**Note:** Since there is no protocol to derive this address, 0.0.0.0 is not permitted.)
- You can specify a **Filter Set**. For more information see Chapter 13, "Security."
- You can remove a **Filter Set**.
- You can choose to configure **Advanced IP Profile Options** (see "Advanced IP Profile Options," in the

following section).

Note: The SPI title field above changes to **SPI (Security Parameters Index) – Use Advanced IP Profile Options** if any of the SPI values differ from each other.

Advanced IP Profile Options

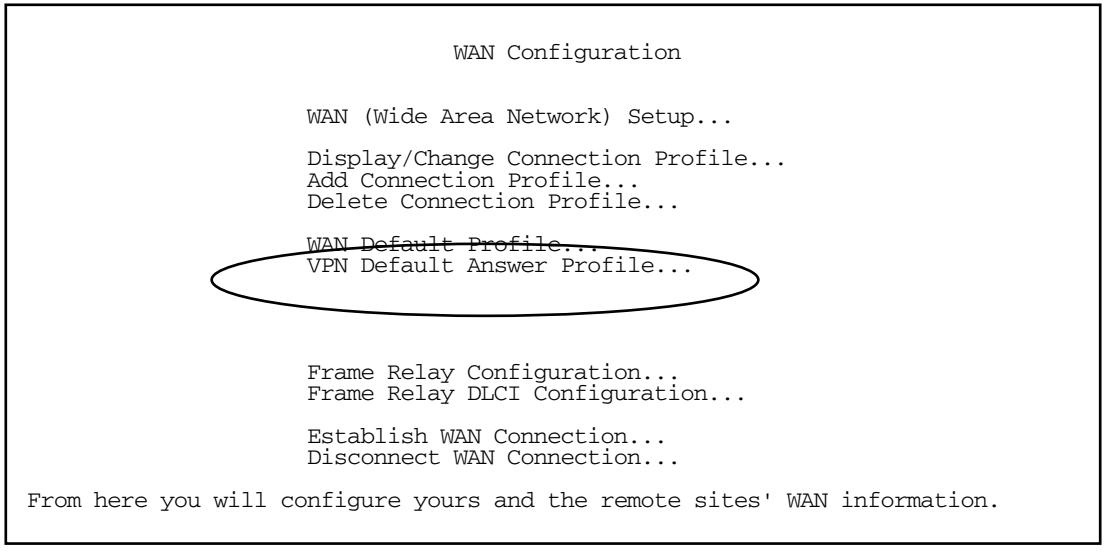


- You can specify an **ESP Receive SPI**. The value must be unique over the set of all ESP SPIs specified for the remote tunnel endpoint.
- You can specify an **ESP Transmit SPI**. The value must be unique over the set of all ESP SPIs specified for the remote tunnel endpoint.
- You can specify an **AH Receive SPI** if AH authentication has been requested. The value must be unique over the set of all AH SPIs specified for the router.
- You can specify an **AH Transmit SPI** if AH authentication has been requested. The value must be unique over the set of all AH SPIs specified for the remote tunnel endpoint.
- You can specify a **Local Tunnel Endpoint Address**. If not 0.0.0.0, this value must be one of the assigned interface addresses, either WAN or LAN. This is used as the source address of all IPsec traffic.
- You can specify a **Next Hop Gateway**. If you specify the Remote Tunnel Endpoint Address, and the address is in the same subnet as the Remote Members Network you specified in the IP Profile Parameters, the **Next Hop Gateway** option allows you to enter the address by which the gateway partner is reached.

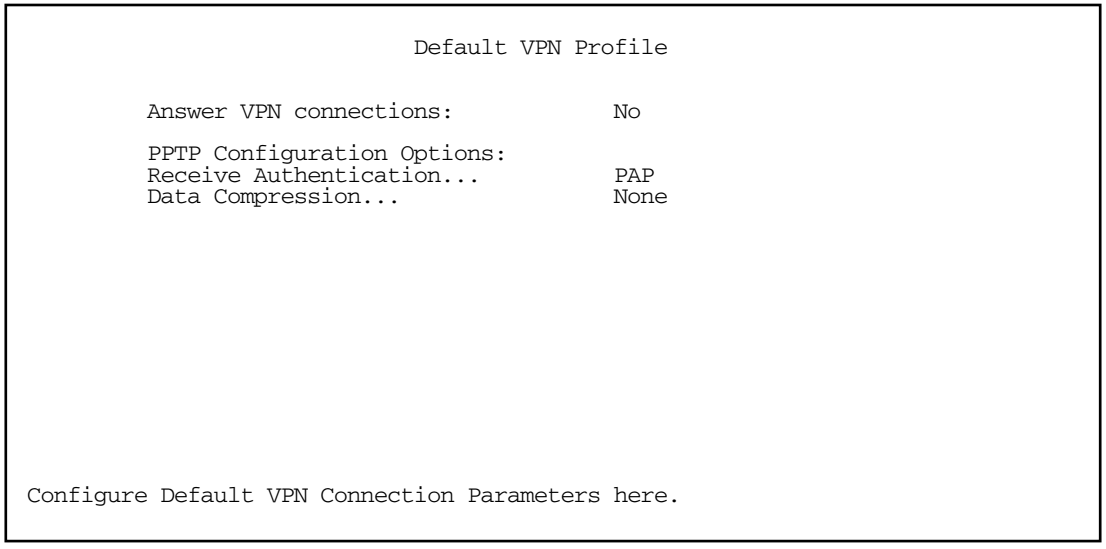
  If you do not specify the Remote Tunnel Endpoint Address, the router will use the default gateway to reach the partner. If the partner should be reached via an alternate port (for example, the LAN instead of the WAN), the **Next Hop Gateway** field allows this path to be resolved.

VPN Default Answer Profile

The WAN Configuration menu offers a VPN Default Answer Profile option. Use this selection when your router is acting as the server for VPN connections, that is, when you are on the answering end of the tunnel establishment. The VPN Default Answer Profile determines the way the attempted tunnel connection is answered.



To set the parameters under which the router will answer attempted VPN connections, select **VPN Default Answer Profile** and press Return. The Default VPN Profile screen appears.



- Toggle **Answer VPN Connections** to **Yes** if you want the router to accept VPN connections or **No** (the default) if you do not. This applies to both ATMP and PPTP connections.

- For PPTP tunnel connections only, you must define what type of authentication these connections will use. Select **Receive Authentication** and press Return. A pop-up menu offers the following options: PAP (the default), CHAP, or MS-CHAP.
- If you chose PAP or CHAP authentication, from the **Data Compression** pop-up menu select either None (the default) or Standard LZS.

  If you chose MS-CHAP authentication, the **Data Compression** option is not required, and this menu item becomes hidden.

Interoperation with other features

- Address serving is not supported through IPsec Tunnels.
- AH is not supported through an interface that has NAT applied to it. NAT may be applied to the inner payload.

  AH is not supported through an interface which is either Unnumbered or Numbered with a dynamically assigned address unless the Local Tunnel Endpoint address is specified in the Advanced IP Profile Options screen.

VPN QuickView

You can view the status of your VPN connections in the VPN QuickView screen.

From the Main Menu select QuickView and then VPN QuickView.

The VPN QuickView screen appears.

```
                              VPN Quick View

Profile Name----------Type--Rx Pckts--Tx Pckts------Est.-Partner Address------
HA <-> FA1 (Jony Fon  ATMP        99        99      Rmt  173.166.82.8
HA <-> FA3 (Sleve M.  ATMP        13        14      Rmt  63.193.117.91
```

Profile Name: Lists the name of the Connection Profile being used, if any.

Type: Shows the data link encapsulation method (PPTP or ATMP).

Rx Pckts: Shows the number of packets received via the VPN tunnel.

Tx Pckts: Shows the number of packets transmitted via the VPN tunnel.

Est: Indicates whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.

Partner Address: Shows the tunnel partner’s IP address.

Dial-Up Networking for VPN

Microsoft Windows Dial-Up Networking software permits a remote standalone workstation to establish a VPN tunnel to a PPTP server such as a Netopia Router located at a central site. Dial-Up Networking also allows a mobile user who may not be connected to a PAC to dial into an intermediate ISP and establish a VPN tunnel to, for example, a corporate headquarters, remotely. Netopia Routers also can serve as a PAC at the workstation's site, making it unnecessary for the standalone workstation to initiate the tunnel. In such a case, the Dial-Up Networking software is not required, since the Netopia Router initiates the tunnel.

This section is provided for users who may require the VPN client software for Dial-Up Networking in order to connect to an ISP who provides a PPTP account.

Microsoft Windows Dial-Up Networking (DUN) is the means by which you can initiate a VPN tunnel between your individual remote client workstation and a private network such as your corporate LAN via the Internet. DUN is a software adapter that allows you to establish a tunnel.

DUN is a free add-on available for Windows 95, and comes standard with Windows 98 and Windows NT. The VPN tunnel behaves as a private network connection, unrelated to other traffic on the network. Once you have installed Dial-Up Networking, you will be able to connect to your remote site as if you had a direct private connection, regardless of the intervening network(s) through which your data passes. You may need to install the Dial-Up Networking feature of Windows 95, 98, or 2000 to take advantage of the virtual private networking feature of your Netopia router.

Note: For the latest information and tech notes on Dial-Up Networking and VPNs be sure to visit the Netopia website at http://www.netopia.com and, for the latest software and release notes, the Microsoft website at http://www.microsoft.com.

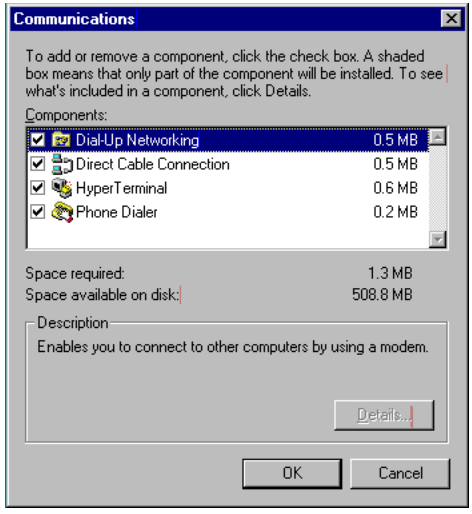
Installing Dial-Up Networking

Check to see if Dial-Up Networking is already installed on your PC. Open your My Computer (or whatever you have named it) icon on your desktop. If there is a folder named Dial-Up Networking, you don't have to install it. If there is no such folder, you must install it from your system disks or CD-ROM. Do the following:

1. From the **Start** menu, select **Settings** and then **Control Panel**.
2. In the Control Panel window, double-click the **Add/Remove Programs** icon.

   The Add/Remove Programs Properties window appears.
3. Click the **Windows Setup** tab.
4. Double-click **Communications**.

The Communications window appears.



5. In the Communications window, select **Dial-Up Networking** and click the **OK** button.

   This returns you to the Windows Setup screen. Click the **OK** button.

6. Respond to the prompts to install Dial-Up Networking from the system disks or CD-ROM.

7. When prompted, reboot your PC.

Creating a new Dial-Up Networking profile

A Dial-Up Networking profile is like an address book entry that contains the information and parameters you need for a secure private connection. You can create this profile by using either the Internet Connection Wizard or the Make New Connection feature of Dial-Up Networking. The following instructions tell you how to create the profile with the Make New Connection feature. Do the following:

1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.

   Open the Dial-Up Networking folder, and then double-click **Make New Connection**. The Make New Connection wizard window appears.

2. Type a name for this connection (such as the name of your company or the computer you are dialing into).

   From the pull-down menu, select the device you intend to use for the virtual private network connection. This can be any device you have installed or connected to your PC. Click the **Next** button. A screen appears with fields for you to enter telephone numbers for the computer you want to connect to.

3. Type the directory number or the **Virtual Circuit Identifier** number.

   This number is provided by your ISP or corporate administrator. Depending on the type of device you are using, the number may or may not resemble an ordinary telephone directory number.

4. Click the **Next** button.

   The final window will give you a chance to accept or change the name you have entered for this profile. If you are satisfied with it, click the **Finish** button. Your profile is complete.

Configuring a Dial-Up Networking profile

Once you have created your Dial-Up Networking profile, you configure it for TCP/IP networking to allow you to connect to the Internet through your Internet connection device. Do the following:

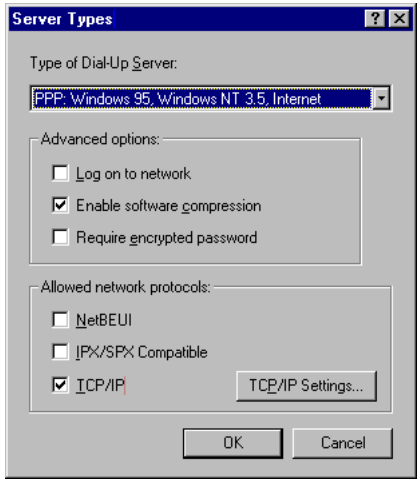
1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.

   Open the Dial-Up Networking folder. You will see the icon for the profile you created in the previous section.

2. Right-click the icon and from the pop-up menu select **Properties**.

3. In the Properties window click the **Server Type** button.

   From the Type of Dial-up Server pull-down menu select the appropriate type of server for your system version:

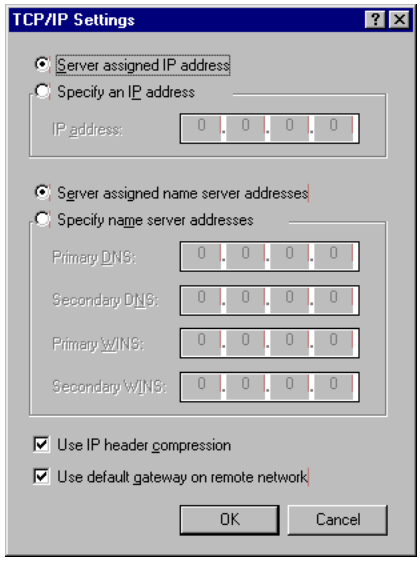


   - Windows 95 users select **PPP: Windows 95, Windows NT 3.5, Internet**
   - Windows 98 users select **PPP: Windows 98, Windows NT Server, Internet**

   In the Allowed network protocols area check **TCP/IP** and uncheck all of the other checkboxes.

   Note: Netopia's PPTP implementation does not currently support tunnelling of IPX and NetBEUI protocols.

4. Click the **TCP/IP Settings** button.



- If your ISP uses dynamic IP addressing (DHCP), select the Server assigned IP address radio button.
- If your ISP uses static IP addressing, select the Specify an IP address radio button and enter your assigned IP address in the fields provided. Also enter the IP address in the Primary and Secondary DNS fields.

5. Click the **OK** button in this window and the next two windows.

Installing the VPN Client

Before installing the VPN Client you must have TCP/IP installed and have an established Internet connection.

Windows 95 VPN installation

1. From your Internet browser navigate to the following URL:

   http://www.microsoft.com/NTServer/nts/downloads/recommended/dunl3win95/releasenotes.aso

   Download the Microsoft Windows 95 VPN patch dun 1.3 to the Windows 95 computer you intend to use as a VPN client with PPTP. Follow the installation instructions.

2. From the Windows 95 **Start** menu select **Settings**, then **Control Panel** and click once.

   The Control Panel screen appears.

3. Double-click **Add/Remove Programs**.

   The Add/Remove Programs screen appears.

4. Click the **Windows Setup** tab.

   The Windows Setup screen will be displayed within the top center box.

5. Highlight **Communications** and double-click.

   This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.

6. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.

7. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.

8. Double-click the **My Computer** icon (normally at the left upper corner of the screen).

   This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.

9. Double-click **Make New Connection**.

   This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.

   Click the **Next** button at the bottom of the screen

   This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Windows 98 VPN installation

1. From the Windows 98 **Start** menu select **Settings**, then **Control Panel** and click once.

   The Control Panel screen appears.

2. Double-click **Add/Remove Programs**.

   The Add/Remove Programs screen appears.

3. Click the **Windows Setup** tab.

   The Windows Setup screen will be displayed within the top center box.

4. Double-click **Communications**.

   This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.

5. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.

6. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.

7. Double-click the **My Computer** icon (normally at the left upper corner of the screen).

   This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.

8. Double-click **Make New Connection**.

   This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.

   Click the **Next** button at the bottom of the screen

   This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Connecting using Dial-Up Networking

A Dial-Up Networking connection will be automatically launched whenever you run a TCP/IP application, such as a Web browser or email client. When you first run the application a Connect To dialog box appears in which you enter your User name and Password. If you check the Save password checkbox, the system will remember your User name and Password, and you won't be prompted for them again.

About ATMP Tunnels

To set up an ATMP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote ATMP partner. ATMP uses the terminology of a *foreign agent* that initiates tunnels and a *home agent* that terminates them. You use the same procedure to initiate or terminate an ATMP tunnel. Used in this way, the terms *initiate* and *terminate* mean the beginning and end of the tunnel; they do not mean *activate* and *deactivate*.

ATMP is a tunneling protocol, with two basic aspects. Tunnels are created and torn down using a session protocol that is UDP-based. User (or client) data is transferred across the tunnel by encapsulating the client data within Generic Routing Encapsulation (GRE). The GRE data is then routed using standard methods.

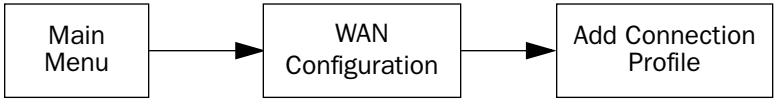
ATMP configuration

ATMP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, since ATMP is not a native encapsulation. The Easy Setup Profile does not offer ATMP datalink encapsulation.

Note: The Netopia R910 Router has access to Connection Profiles for tunnelling purposes. If the PPP dialup kit is not installed, you cannot use PPP as a datalink encapsulation, and have access only to ATMP and PPTP. If the kit is installed you also have access to PPP.

The WAN Event History screens will report VPN tunnel events, such as connections and disconnections, as Channel 4 (and higher) events.

To define an ATMP tunnel, navigate to the **Add Connection Profile** menu from the Main Menu.



```
                        Add Connection Profile

        Profile Name:                     Profile 1
        Profile Enabled:                +--------------+
                                        +--------------+
        Data Link Encapsulation...      | PPP          |
        Data Link Options...            | Frame Relay  |
                                        | ATM FUNI     |
        IP Enabled:                     | ATMP         |
        IP Profile Parameters...        | PPTP         |
                                        +--------------+









        COMMIT                  CANCEL
```

When you define a Connection Profile as using ATMP by selecting ATMP as the datalink encapsulation method, and then select **Data Link Options**, the ATMP Tunnel Options screen appears.

```
                        ATMP Tunnel Options


        ATMP Partner IP Address:          173.167.8.134
        Tunnel Via Gateway:               0.0.0.0

        Network Name:                     sam.net
        Password:                         ****

        Data Encryption...                DES
        Key String:

        Initiate Connections:             Yes
        On Demand:                        Yes

        Idle Timeout (seconds):           300




Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
In this Screen you will configure the GRE/ATMP specific connection params.
```

Note: An ATMP tunnel cannot be assigned a dynamic IP address by the remote server, as in a PPP connection. When you define an ATMP tunnel profile, the Local WAN IP Address, assigned in the IP Profile Parameters screen, must be the true IP address, not 0.0.0.0, if NAT is enabled.

Note: Profiles using ATMP do not offer a Telco Options screen.

- **ATMP Partner IP Address** specifies the address of the other end of the tunnel. When unspecified, the gateway can not initiate tunnels (i.e., act as a foreign agent) for this profile; it can only accept tunnel requests as a home agent.

- When you specify the ATMP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, you can specify the route (**Tunnel Via Gateway**) by which the gateway partner is reached. If you do not specify the ATMP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e., the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.
- You can specify a **Network Name**. When the tunnel partner is another Netopia router, this name may be used to match against a Connection Profile. When the partner is an Ascend router in Gateway mode, then **Network Name** is used by the Ascend router to match a gateway profile. When the partner is an Ascend router in Router mode, leave this field blank.
- You must specify a **Password**, used for authenticating the tunnel.

  Note: The Password entry will be the same for both ends of the tunnel.
- For Netopia-to-Netopia connections only, you can specify a **Data Encryption** algorithm for the ATMP connection from the pop-up menu, either DES or None. None is the default.

  Note: Ascend does not support DES encryption for ATMP tunnels.
- You must specify an 8-byte **Key String** when DES is selected. When encryption is None, this field is invisible.
- You can specify that this router will **Initiate Connections**, acting as a foreign agent (**Yes**), or only answer them, acting as a home agent (**No**).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established through the call management screens.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

```
                          IP Profile Parameters

        Address Translation Enabled:       Yes


        NAT Map List...                    Easy-PAT
        NAT Server List...                 Easy-Servers

        Local WAN IP Address:              0.0.0.0

        Remote IP Address:                 173.167.8.10
        Remote IP Mask:                    255.255.0.0

        Filter Set...
        Remove Filter Set

        Receive RIP:                       Both


Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).
```

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a foreign agent has NAT applied to a Connection Profile set for ATMP data link encapsulation, the home agent and devices behind it, cannot Ping the foreign agent's tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia Router is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

Allowing VPNs through a Firewall

An administrator interested in securing a network will usually combine the use of VPNs with the use of a firewall or some similar mechanism. This is because a VPN is not a complete security solution, but rather a component of overall security. Using a VPN will add security to transactions carried over a public network, but a VPN alone will not prevent a public network from infiltrating a private network. Therefore, you should combine use of a firewall with VPNs, where the firewall will secure the private network from infiltration from a public network, and the VPN will secure the transactions that must cross the public network.

A strict firewall may not be provisioned to allow VPN traffic to pass back and forth as needed. In order to ensure that a firewall will allow a VPN, certain attributes must be added to the firewall's provisioning. The provisions necessary vary slightly between ATMP and PPTP, but both protocols operate on the same basic premise: there are control and negotiation operations, and there is the tunnelled traffic that carries the payload of data between the VPN endpoints. The difference is that ATMP uses UDP to handle control and negotiation, while PPTP uses TCP. Then both ATMP and PPTP use GRE to carry the payload.

For PPTP negotiation to work, TCP packets inbound and outbound destined for port 1723 must be allowed. Likewise, for ATMP negotiation to work, UDP packets inbound and outbound destined for port 5150 must be allowed. Source ports are dynamic, so, if possible, make this flexible, too. Additionally, PPTP and ATMP both require a firewall to allow GRE bi-directionally.

The following sections illustrate a sample filtering setup to allow either PPTP or ATMP traffic to cross a firewall:

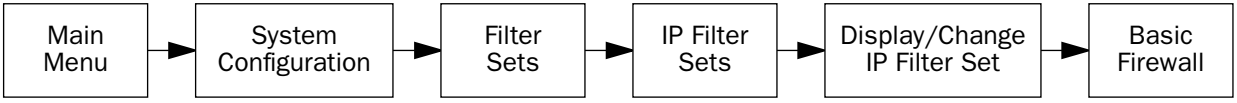
- "PPTP example" on page 10-99
- "ATMP example" on page 10-102

Make your own appropriate substitutions. For more information on filters and firewalls, see Chapter 13, "Security."

PPTP example

To enable a firewall to allow PPTP traffic, you must provision the firewall to allow inbound and outbound TCP packets specifically destined for port 1723. The source port may be dynamic, so often it is not useful to apply a compare function upon this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets, enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0          0.0.0.0          TCP   NC       =1723    Yes Yes |
| 2    0.0.0.0          0.0.0.0          GRE   --       --       Yes Yes |
|                                                                         |
```

For Input Filter 1 set the Destination Port information as shown below.

```
                        Change Input Filter 1

      Enabled:                          Yes
      Forward:                          Yes


      Source IP Address:                0.0.0.0
      Source IP Address Mask:           0.0.0.0

      Dest. IP Address:                 0.0.0.0
      Dest. IP Address Mask:            0.0.0.0

      Protocol Type:                    TCP
      Source Port Compare...            No Compare
      Source Port ID:                   0
      Dest. Port Compare...             Equal
      Dest. Port ID:                    1723
      Established TCP Conns. Only:      No
```

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

```
                        Change Input Filter 2

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      GRE
```

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0           0.0.0.0           TCP   NC       =1723   Yes Yes |
| 2    0.0.0.0           0.0.0.0           GRE   --       --      Yes Yes |
```

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

```
                        Change Output Filter 1

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      TCP
        Source Port Compare...              No Compare
        Source Port ID:                     0
        Dest. Port Compare...               Equal
        Dest. Port ID:                      1723
        Established TCP Conns. Only:        No
```

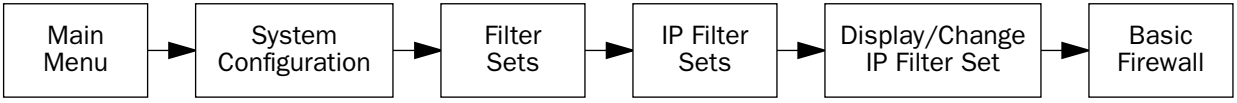
For Output Filter 2 set the Protocol Type to allow GRE as shown below.

```
                    Change Output Filter 2

Enabled:                              Yes
Forward:                              Yes


Source IP Address:                    0.0.0.0
Source IP Address Mask:               0.0.0.0

Dest. IP Address:                     0.0.0.0
Dest. IP Address Mask:                0.0.0.0

Protocol Type:                        GRE
```

ATMP example

To enable a firewall to allow ATMP traffic, you must provision the firewall to allow inbound and outbound UDP packets specifically destined for port 5150. The source port may be dynamic, so often it is not useful to apply a compare function on this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets (Protocol 47, Internet Assigned Numbers Document, RFC 1700), enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0           0.0.0.0           UDP   NC       =5150   Yes Yes |
| 2    0.0.0.0           0.0.0.0           GRE   --       --      Yes Yes |
|                                                                         |
```

For Input Filter 1 set the Destination Port information as shown below.

```
                        Change Input Filter 1

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      TCP
        Source Port Compare...              No Compare
        Source Port ID:                     0
        Dest. Port Compare...               Equal
        Dest. Port ID:                      1723
        Established TCP Conns. Only:        No
```

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

```
                        Change Input Filter 2

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      GRE
```

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

```
+-#----Source IP Addr----Dest IP Addr------Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1    0.0.0.0           0.0.0.0           UDP   NC       NC       Yes Yes |
| 2    0.0.0.0           0.0.0.0           GRE   --       --       Yes Yes |
|                                                                         |
```

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

```
                        Change Output Filter 1

        Enabled:                            Yes
        Forward:                            Yes


        Source IP Address:                  0.0.0.0
        Source IP Address Mask:             0.0.0.0

        Dest. IP Address:                   0.0.0.0
        Dest. IP Address Mask:              0.0.0.0

        Protocol Type:                      UDP
        Source Port Compare...              No Compare
        Source Port ID:                     0
        Dest. Port Compare...               No Compare
        Dest. Port ID:                      5150
```

For Output Filter 2 set the Protocol Type to allow GRE as shown below.

```
                    Change Output Filter 2

Enabled:                              Yes
Forward:                              Yes


Source IP Address:                    0.0.0.0
Source IP Address Mask:               0.0.0.0

Dest. IP Address:                     0.0.0.0
Dest. IP Address Mask:                0.0.0.0

Protocol Type:                        GRE
```

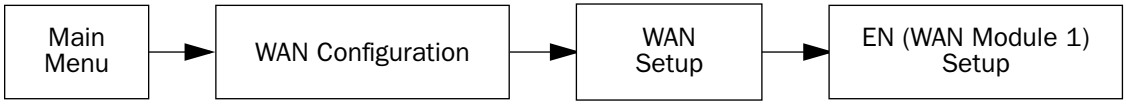
Chapter 11

PPP over Ethernet

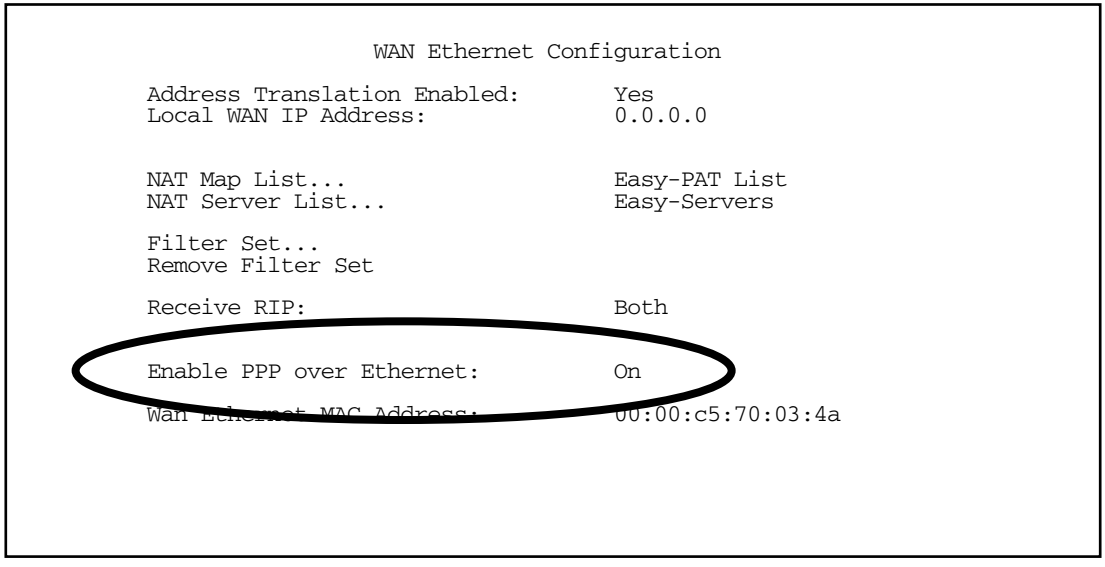
The Netopia R910 Router supports the Point-to-Point protocol over Ethernet (PPPoE) for use of PPP to connect through a DSL or cable modem. Some ISPs require user name and password authentication to connect you with their DSL or cable service. PPPoE allows user name and password authentication to the ISP via your R910's Ethernet interface to your DSL or cable modem.

To configure PPP authentication in your R910, you first enable PPP over Ethernet and then create a Connection Profile for your Internet connection.

From the **Main Menu** select **WAN Configuration**, **WAN Setup**, and then **EN (Wan Module 1) Setup**. Press **Return**.



The WAN Ethernet Configuration screen appears.



Toggle **Enable PPP over Ethernet** to **On**, using the Tab key. Press **Return**, and then **Escape** twice to return to **WAN Configuration**. Select **Add Connection Profile**. Press **Return**.

The **Add Connection Profile** screen appears.

```
                          Add Connection Profile

        Profile Name:                          My_ISP
        Profile Enabled:                       Yes

        Data Link Encapsulation...             PPP
        Data Link Options...

        IP Enabled:                            Yes
        IP Profile Parameters...



        Interface Group...                     Primary



        COMMIT                      CANCEL

Configure a new Conn. Profile. Finished?  ADD or CANCEL to exit.
```

From the **Data Link Encapsulation** pop-up menu, select **PPP**.

Select **Data Link Options** and press **Return**.

The **Datalink (PPP/MP) Options** screen appears.

```
                        Datalink (PPP/MP) Options

        Data Compression...                    Standard LZS

        Send Authentication...                 PAP

        Send User Name:                        jagdip
        Send Password:                         *****

        Receive User Name:
        Receive Password:

        Dial...                                Dial In/Out
        Dial on Demand:                        Yes

        Idle Timeout (seconds):                300

        Maximum Packet Size:                   1500

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
```

Enter your User Name and Password and press **Return**. Press **Escape** to return to the Add Connection Profile screen.

Select **ADD PROFILE NOW** and press **Return**. Your Connection Profile will be created and activated with your authentication information to connect to your ISP's service.

PPP Ethernet LAN Reconfiguration

The Netopia R910 offers the ability for PPP to reconfigure the router's Ethernet LAN when establishing an unnumbered, non-NAT connection.

The Netopia R910 allows a central site router to supply an entire IP subnet, rather than a single IP address, for use by a Netopia router. If the applicable Connection Profile specifies an unnumbered, non-NAT connection and Negotiate LAN IP Addr/Mask is set to On, PPP will attempt to negotiate both an IP Address and subnet mask.

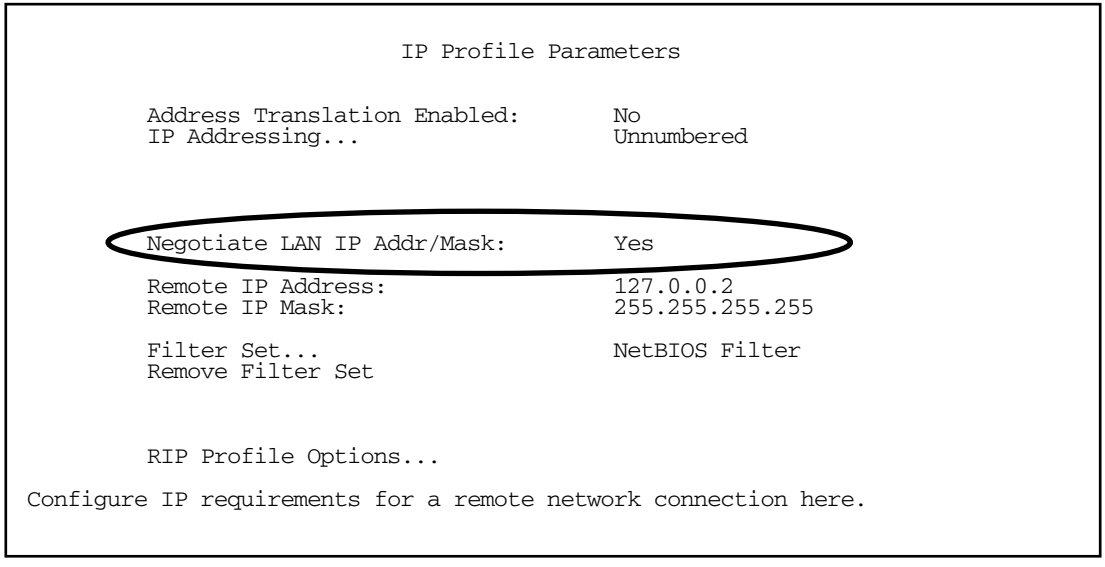
Note: Once the router has reconfigured the address serving pool only to conform to the negotiated subnet, you can adjust the base or extent of the pool and reboot the router. Your adjustments will not be overwritten when the connection is next renegotiated because the router only reconfigures the address serving pool if it lies outside the negotiated subnet.

The router does not adjust any address serving parameters other than the base and extent of the address serving pool. This allows you to otherwise configure address serving as you please using the normal address serving configuration items. For example, if you disable address serving, the router will not enable address serving when it reconfigures the address serving pool.

Configuration

To enable PPP Ethernet LAN configuration, navigate to the IP Profile Parameters screen of the Connection Profile you want to use. This can be either the Easy Setup Profile or any other Connection Profile you have added.

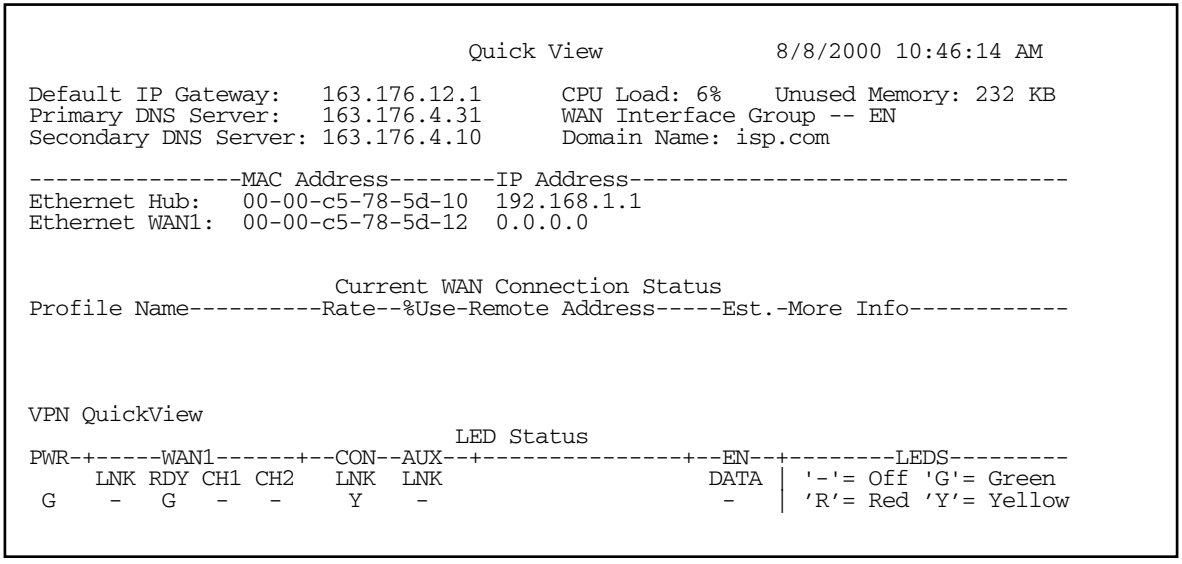
The IP Profile Parameters screen for a Connection Profile displays a Negotiate LAN IP Addr/Mask toggle:



- This toggle is visible only if the profile's Data Link Encapsulation is set to **PPP**, the Address Translation Enabled toggle is set to **No** and IP Addressing is set to **Unnumbered**. The default value is **No**.
- RIP Profile Options is not visible if Negotiate LAN IP Addr/Mask is set to **Yes** and the Remote IP Mask is set to 0.0.0.0.

Quick View

The Quick View screen (as shown below) displays both Primary and Secondary DNS Server addresses. This is useful because both may be served via PPP.



Chapter 12

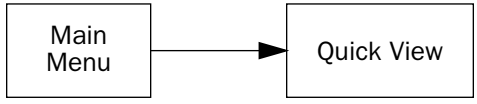
Monitoring Tools

This chapter discusses the Netopia R910's device and network monitoring tools. These tools can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

This section covers the following topics:

Quick View status overview

You can get a useful, overall status report from the Netopia R910 in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.



The Quick View screen has three status sections:

- General status
- Current WAN Connection Status
- LED Status

The status sections vary according to the interface of your Netopia R910.

General status

```
                                  Quick View              12/14/1998 01:13:52 PM

Default IP Gateway:  0.0.0.0              CPU Load: 5%    Unused Memory: 1017 KB
Domain Name Server:  0.0.0.0
Domain Name: netopia.com

----------------MAC Address--------IP Address---------------------------------
Ethernet Hub:   00-00-c5-70-03-48  192.168.1.1
Ethernet WAN1:  00-00-c5-70-03-4a  0.0.0.0









                                     LED Status
PWR-+------ENWAN---------+--EN--+--------LEDS-----------------------------------
      LNK RDY CH1 CH2       DATA | '-'= Off 'G'= Green
 G     -   -   -   -         -   | 'R'= Red 'Y'= Yellow
```

Current Date: The current date; this can be set with the Date and Time utility (see "Date and time" on page 8-47).

Default IP Gateway: Actual IP address of the default gateway, if entered. 0.0.0.0 indicates automatic addressing.

Domain Name Server: IP address of your DNS server.

Domain Name: Domain name you have entered, usually your ISP, such as netopia.com.

CPU Load: Percentage of the system's resources being used by all current transmissions.

Unused Memory: The total remaining system memory available for use.

Ethernet Address: The Netopia R910's hardware address.

IP Address: The Netopia R910's IP address, entered in the IP Setup screen.

Status lights

This section shows the current real-time status of the Netopia R910's status lights (LEDs). It is useful for remotely monitoring the router's status. The Quick View screen's arrangement of LEDs corresponds to the physical arrangement of LEDs on the router.

```
PWR-+------ENWAN----------+--EN--+--------LEDS-----------------------------------
      LNK RDY CH1 CH2       DATA | '-'= Off 'G'= Green
 G     -   -   -   -         -   | 'R'= Red 'Y'= Yellow
```

Each LED representation can report one of four states:

–: A dash means the LED is off.

R: The letter “R” means the LED is red.

G: The letter “G” means the LED is green.

Y: The letter “Y” means the LED is yellow.

The section “Netopia R910 Ethernet Router status lights” on page 3-16 describes the meanings of the colors for each LED.

Note: Although the Quick VIew LED Status section lists the Channel 2 (CH2) LED, it is not used on the R910.

Statistics & Logs

When you are troubleshooting your Netopia R910, the Statistics & Logs screens provide insight into the recent event activities of the router.

From the Main Menu go to **Statistics & Logs** and select one of the options described in the sections below.

General Statistics

To go to the General Statistics screen, select **General Statistics** and press Return. The General Statistics screen appears.

```
                              General Statistics

Phys I/F---------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
Ethernet Hub     123456789  123456789  12345678  12345678  12345678  12345678
Ethernet Wan1    123456789  123456789  12345678  12345678

Network----------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
IP               123456789  123456789  12345678  12345678  12345678  12345678
```

The General Statistics screen displays information about data traffic on the Netopia R910’s data ports. This information is useful for monitoring and troubleshooting your LAN. Note that the counters roll over at their maximum field width, that is, they restart again at 0.

Physical Interface

The top left side of the screen lists total packets received and total packets transmitted for the following data ports:

- Ethernet Hub
- Ethernet WAN

Network Interface

The bottom left side of the screen lists total packets received and total packets transmitted for the IP protocol (IP packets on the Ethernet)

The right side of the table lists the total number of occurrences of each of six types of communication statistics:

Rx Bytes. The number of bytes received

Tx Bytes. The number of bytes transmitted

Rx Packets: The number of packets received

Tx Pkts. The number of packets transmitted

Rx Err: The number of bad Ethernet packets received

Tx Err: An error occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN

Event histories

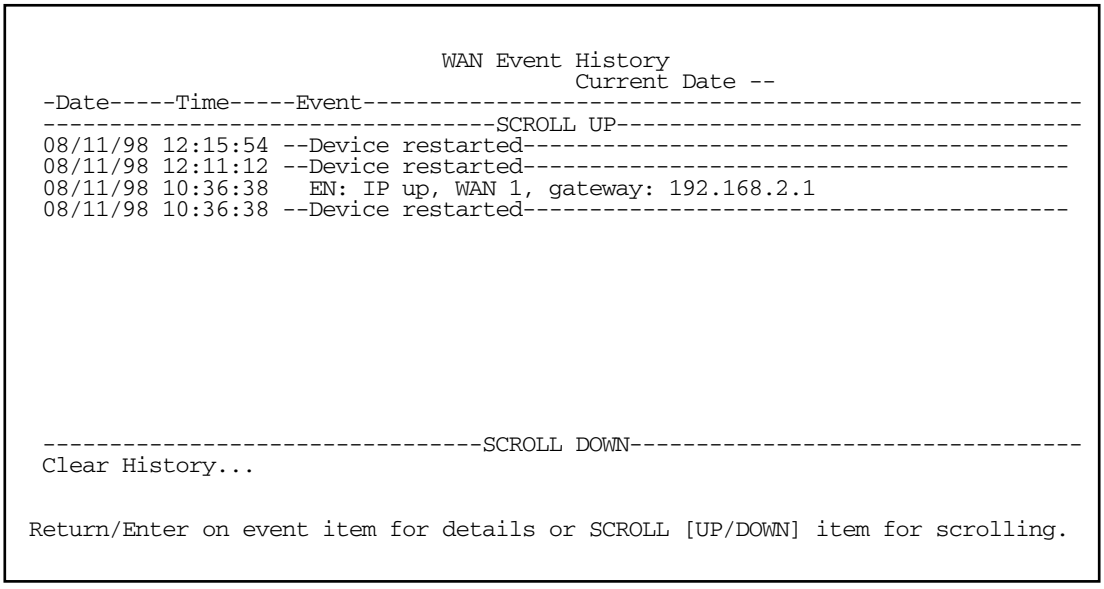
The Netopia R910 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R910's built-in battery backup prevents loss of event history from a shutdown or reset.

The router's event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History retain records of the 128 most recent events.

In the Statistics & Logs screen, select **WAN Event History**. The WAN Event History screen appears.

WAN Event History

The WAN Event History screen lists a total of 128 events on the WAN. The most recent events appear at the top.



Each entry in the list contains the following information:

Date: Date of the event.

Time: Time of the event.

Event: A brief description of the event.

The first event in each call sequence is marked with double arrows (>>).

Failures are marked with an asterisk (*).

If the event history exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To get more information about any event listed in the WAN Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or Escape to dismiss the dialog box.

To clear the event history, select **Clear History** at the bottom of the history screen and press Return.

Device Event History

The Device Event History screen lists a total of 128 port and system events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

In the Statistics & Logs screen, select **Device Event History**. The Device Event History screen appears.

```
                          Device Event History
                                        Current Date --  12/11/98 12:26:39 PM
 -Date-----Time-----Event-----------------------------------------------------
 ---------------------------------SCROLL UP-------------------------------------
 08/11/98 12:25:28   Telnet connection up, address 163.176.8.134
 08/11/98 12:25:05 * IP address server configuration error; server disabled
 08/11/98 12:25:05 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:25:05 --BOOT: Warm start v4.8 ---------------------------------
 08/11/98 12:19:17 * IP address server configuration error; server disabled
 08/11/98 12:19:17 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:19:17 --BOOT: Warm start v4.8 ---------------------------------
 08/11/98 12:18:15 * IP address server configuration error; server disabled
 08/11/98 12:18:15 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:18:15 --BOOT: Warm start v4.8 ---------------------------------
 08/11/98 12:16:34   Telnet connection up, address 163.176.8.134
 08/11/98 12:15:54   IP address server initialization complete
 08/11/98 12:15:54 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:15:54 --BOOT: Warm start v4.8 ---------------------------------
 -------------------------------SCROLL DOWN-------------------------------------
 Clear History...

Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

If the event history exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To obtain more information about any event listed in the Device Event History, select the event and then press Return. A dialog box containing more information about the selected event appears. Press Return or Escape to dismiss the dialog box.

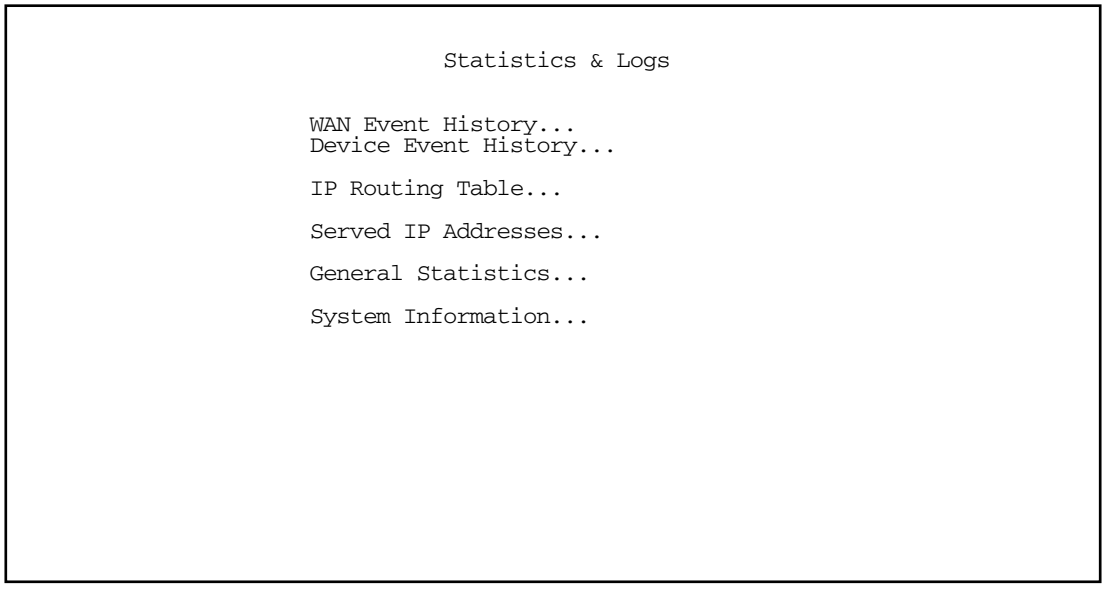
To clear the Device Event History, select **Clear History** and press Return.

Routing tables

You can view all of the IP routes in the Netopia R910's IP routing table.

To go to a routing table screen, select the IP routing table from the **Statistics & Logs** screen.

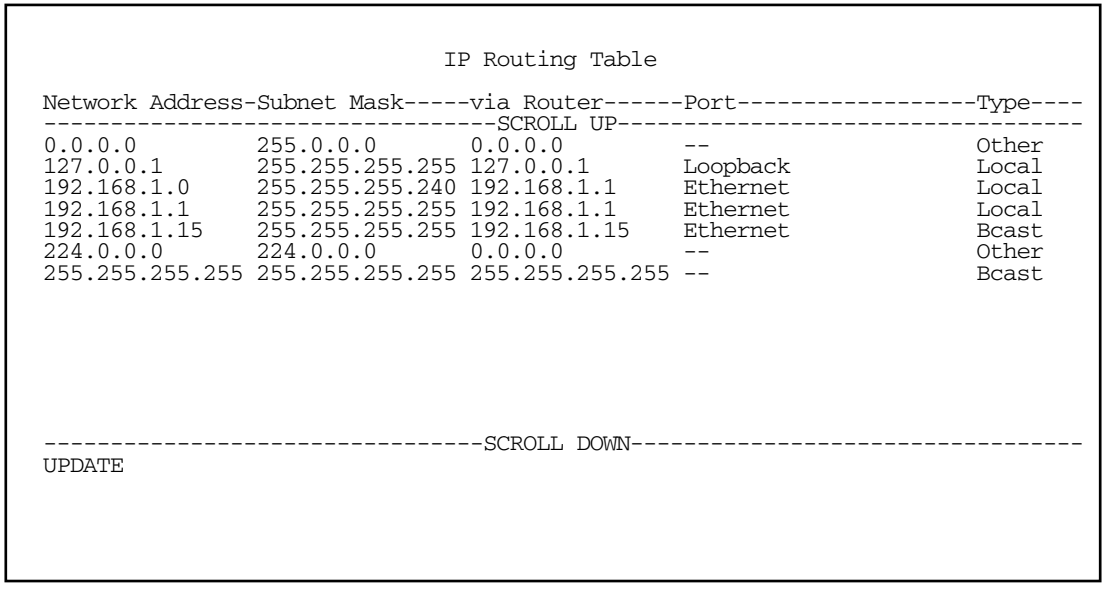
Each of the routing table screens represents a "snapshot" of the routing table information at the time the screen is first invoked. To take a new snapshot, select **Update** at the bottom of the screen and press Return.



IP routing table

In the Statistics & Logs screen, select **IP Routing Table** and press Return.

The IP routing table displays all of the IP routes currently known to the Netopia R910.



If the list of routes shown exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the table and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the table and press Return.

Served IP Addresses

You can view all of the IP addresses currently being served by the Netopia R910 Ethernet Router from the **Served IP Addresses** screen.

From the Statistics & Logs menu, select **Served IP Addresses**. The Served IP Addresses screen appears.

```
                          Served IP Addresses

-IP Address-------Type----Expires--Client Identifier--------------------------
---------------------------------SCROLL UP-----------------------------------
 192.168.1.100    DHCP    00:36    EN: 00-00-c5-4a-1f-ea
 192.168.1.101    DHCP    00:58    EN: 08-00-07-16-0c-85
 192.168.1.102
 192.168.1.103
 192.168.1.104
 192.168.1.105
 192.168.1.106
 192.168.1.107
 192.168.1.108
 192.168.1.109
 192.168.1.110
 192.168.1.111
 192.168.1.112
 192.168.1.113
---------------------------------SCROLL DOWN---------------------------------
Lease Management...

  EN = Ethernet Address; AT = AppleTalk Address; CP = Profile Name; HX = hex
```

To manage DHCP leases, select **Lease Management** in this screen.

The IP Address Lease Management screen appears.

```
                       IP Address Lease Management

        Reset All Leases

        Release BootP Leases

        Reclaim Declined Addresses









Hit RETURN/ENTER, you will return to the previous screen.
```

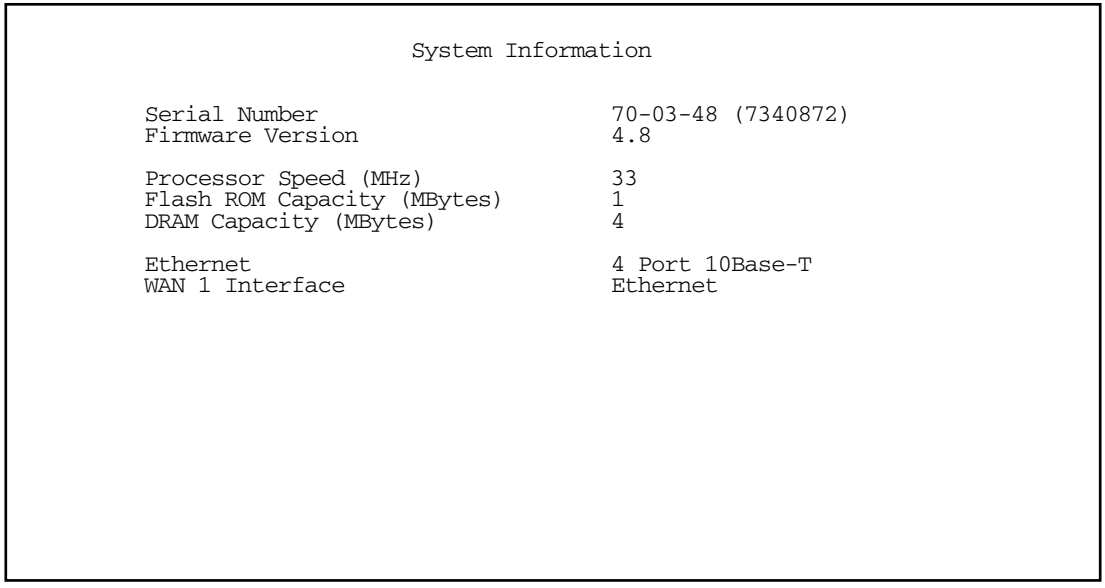
This screen has three options:

- **Reset All Leases**: Resets all current IP addresses leased through DHCP without waiting for the default one–hour lease period to elapse
- **Release BootP Leases**: Releases any BootP leases that may be in place, and which may no longer be required.
- **Reclaim Declined Addresses**: Reclaims served leases that have been declined; for example by devices that may no longer be on the network.

System Information

The System Information screen gives a summary view of the general system level values in the Netopia R910 Ethernet Router.

From the Statistics & Logs menu select **System Information**. The System Information screen appears.



The information display varies by model, firmware version, feature set, and so on. You can tell at a glance your particular system configuration.

SNMP

The Netopia R910 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

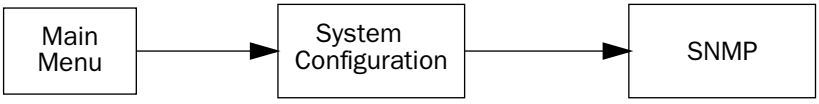
The Netopia R910 supports the following management information base (MIB) documents:

- MIB II (RFC 1213)
- Interface MIB (RFC 1229)
- Ethernet MIB (RFC 1643)
- Netopia MIB

These MIBs are on the Netopia R910 CD included with the Netopia R910. Load these MIBs into your SNMP management software in the order they are listed here. Follow the instructions included with your SNMP manager on how to load MIBs.

The SNMP Setup screen

From the Main Menu, select **SNMP** in the System Configuration screen and press Return. The SNMP Setup screen appears.




```
                              SNMP Setup

          System Name:
          System Location:
          System Contact:


          Read-Only Community String:        public
          Read/Write Community String:       private

          Authentication Traps Enable:       Off

          IP Trap Receivers...




 Configure optional SNMP parameters from here.
```

Follow these steps to configure the first three items in the screen:

1. Select **System Name** and enter a descriptive name for the Netopia R910's SNMP agent.

2. Select **System Location** and enter the router's physical location (room, floor, building, etc.).
3. Select **System Contact** and enter the name of the person responsible for maintaining the router.

System Name, System Location, and System Contact set the values returned by the Netopia R910 SNMP agent for the SysName, SysLocation, and SysContact objects, respectively, in the MIB II system group. Although optional, the information you enter in these items can help a system administrator manage the network more efficiently.

Community strings

The **Read-Only Community String** and the **Read/Write Community String** are like passwords that must be used by an SNMP manager querying or configuring the Netopia R910. An SNMP manager using the **Read-Only Community String** can examine statistics and configuration information from the router, but cannot modify the router's configuration. An SNMP manager using the **Read/Write Community String** can both examine and modify configuration parameters.

By default, the read-only community string is set to "public" and the read/write community string is blank. You should change both of the default community strings to values known only to you and trusted system administrators.

Setting the Read-Only and Read-Write community strings to the empty string will block all SNMP requests to the router. (The router may still send SNMP Traps if those are properly enabled.)

Previously, if either community string was the empty string, SNMP Requests specifying an empty community string were accepted and processed.

This change is designed to allow the administrator to block SNMP access to the router, and to provide more granular control over the allowed SNMP operations to the router.

- Setting only the Read-Write community string to the empty string will block SNMP Set Requests to the router, but Get Requests and Get-Next Requests will still be honored using the Read-Only community string (assuming that is not the empty string).
- Setting only the Read-Only community string to the empty string will *not* block Get Requests or Get-Next Requests since those operations (and Set Requests) are still allowed using the (non-empty) Read-Write community string.

To change a community string, select it and enter a new value.

Caution! Even if you decide not to use SNMP, you should change the read-only community string and leave the read/write community string blank. This prevents unauthorized access to the Netopia R910 through SNMP. For more information on security issues, see "Suggested security measures" on page 13-123.

SNMP traps

An SNMP **trap** is an informational message sent from an SNMP agent (in this case, the Netopia R910) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

Standard traps generated by the Netopia R910 include the following:

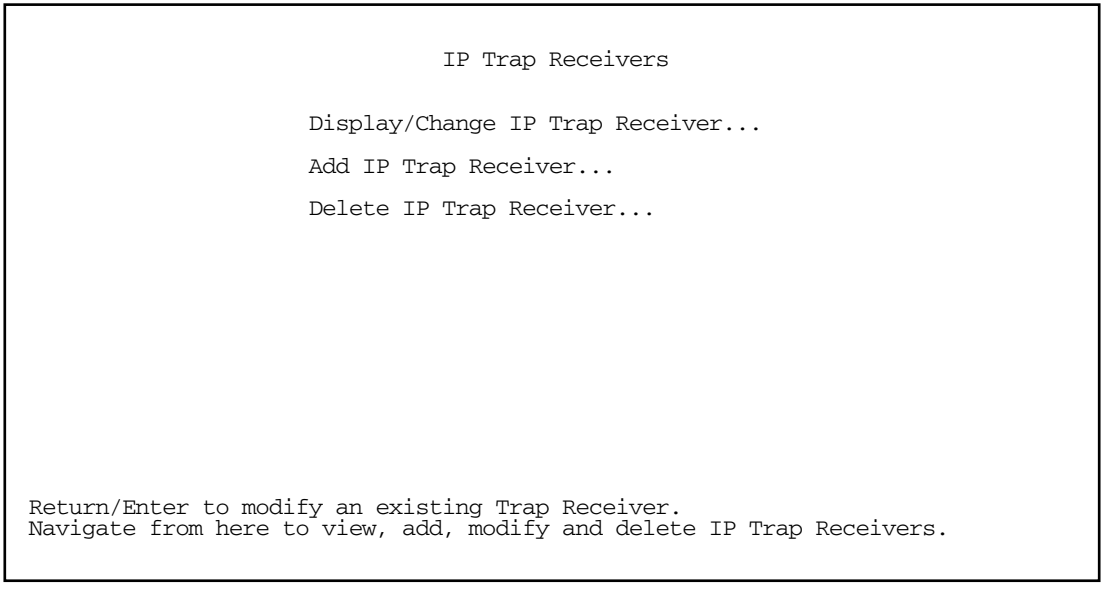
- An authentication failure trap is generated when the router detects an incorrect community string in a received SNMP packet. **Authentication Traps Enable** must be **On** for this trap to be generated.

- A cold start trap is generated after the router is reset.
- An interface down trap (ifDown) is generated when one of the router's interfaces, such as a port, stops functioning or is disabled.
- An interface up trap (ifUp) is generated when one of the router's interfaces, such as a port, begins functioning.

The Netopia R910 sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia R910. Up to eight receivers can be set. You can also review and remove IP traps.

To go to the IP Trap Receivers screen, select **IP Trap Receivers**. The IP Trap Receivers screen appears.



Setting the IP trap receivers

1. Select **Add IP Trap Receiver**.
2. Select **Receiver IP Address or Domain Name**. Enter the IP address or domain name of the SNMP manager you want to receive the trap.
3. Select **Community String**. Enter whatever community string is appropriate for the traps to be sent to the management station whose IP address or domain name you entered on the previous line.
4. Select **Add Trap Receiver Now** and press Return. You can add up to seven more receivers.

Viewing IP trap receivers

To display a view-only table of IP trap receivers, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.

Modifying IP trap receivers

1. To edit an IP trap receiver, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.

2. Select an IP trap receiver from the table and press Return.
3. In the **Change IP Trap Receiver** screen, edit the information as needed and press Return.

Deleting IP trap receivers

1. To delete an IP trap receiver, select **Delete IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the dialog box, select **Continue** and press Return.

Chapter 13

Security

The Netopia R910 provides a number of security features to help protect its configuration screens and your local network from unauthorized access. Although these features are optional, it is strongly recommended that you use them.

This section covers the following topics:

Suggested security measures

In addition to setting up user accounts, Telnet access, and filters (all of which are covered later in this chapter), there are other actions you can take to make the Netopia R910 and your network more secure:

- Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.
- Set the answer profile so it must match incoming calls to a connection profile.
- Set the Enable Dial-in Console Access option to No.
- When using AURP, accept connections only from configured partners.
- Configure the Netopia R910 through the serial console port to ensure that your communications cannot be intercepted.

User accounts

When you first set up and configure the Netopia R910, no passwords are required to access the configuration screens. Anyone could tamper with the router's configuration by simply connecting it to a console.

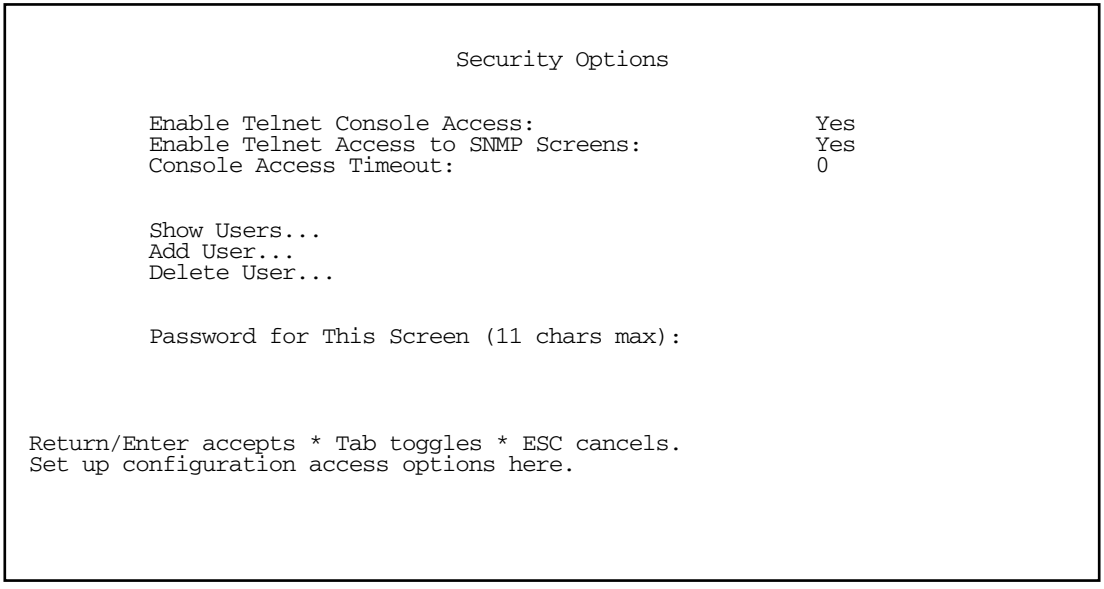
However, by adding user accounts, you can protect the most sensitive screens from unauthorized access. User accounts are composed of name/password combinations that can be given to authorized users.

Caution!

You are strongly encouraged to add protection to the configuration screens. Unprotected screens could allow an unauthorized user to compromise the operation of your entire network.

Once user accounts are created, users who attempt to access protected screens will be challenged. Users who enter an incorrect name or password are returned to a screen requesting a name/password combination to access the Main Menu.

To set up user accounts, in the System Configuration screen select **Security** and press Return. The Security Options screen appears.



Protecting the Security Options screen

The first screen you should protect is the Security Options screen, because it controls access to the configuration screens. Access to the Security Options screen can be protected with a password.

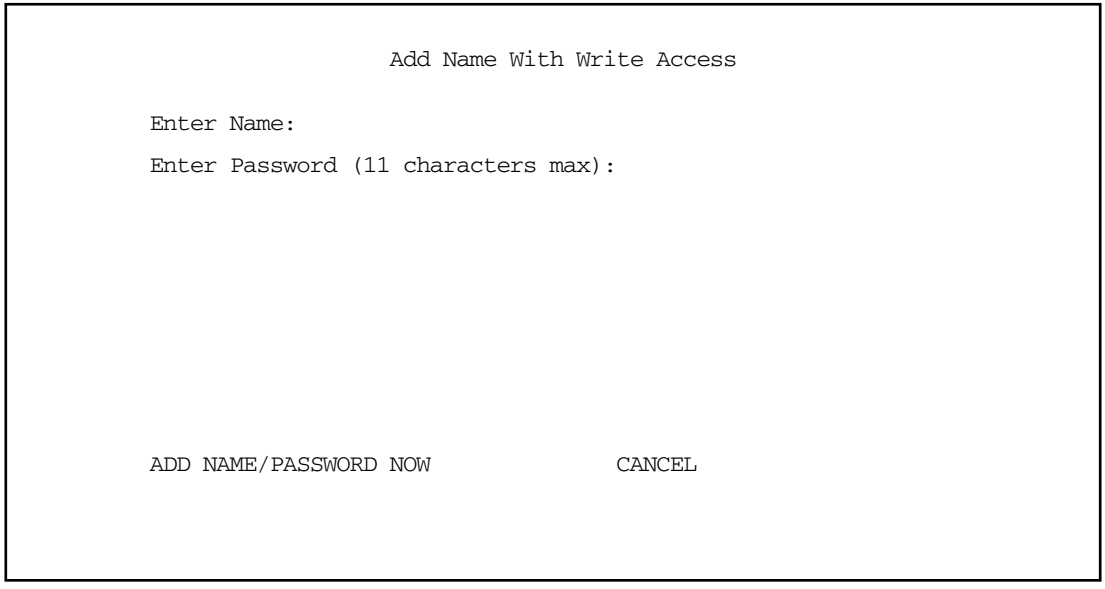
Select **Password for This Screen** in the Security Options screen and enter a password. Make sure this password is secure and is different from any of the user account passwords.

Protecting the configuration screens

You can protect the configuration screens with user accounts. You can administer the accounts from the Security Options screen. You can create up to four accounts.

To display a view-only list of user accounts, select **Show Users** in the Security Options screen.

To add a new user account, select **Add User** in the Security Options screen and press Return. The Add Name With Write Access screen appears.



Follow these steps to configure the new account:

1. Select **Enter Name** and enter a descriptive name (for example, the user's first name).
2. Select **Enter Password** and enter a password.
3. To accept the new name/password combination, select **ADD NAME/PASSWORD NOW**. To exit the Add Name With Write Access screen without saving the new account, select **CANCEL**. You are returned to the Security Options screen.

To delete a user account, select **Delete User** to display a list of accounts. Select an account from the list and press Return to delete it. To exit the list without deleting the selected account, press Escape.

Telnet access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. The Netopia R910 supports Telnet access to its configuration screens.

Caution!

You should consider password-protecting or restricting Telnet access to the Netopia R910 if you suspect there is a chance of tampering.

To password-protect the configuration screens, select Easy Setup from the Main Menu, and go to the **Easy Setup Security Configuration** screen. By entering a name and password pair in this screen, all access via serial, Telnet, SNMP, and Web server will be password-protected.

To restrict Telnet access, select **Security** in the Advanced Configuration menu. The Security Options screen will appear. There are two levels of Telnet restriction available:

To restrict Telnet access to the SNMP screens, select **Enable Telnet Access to SNMP Screens** and toggle it to **No**. (See "SNMP traps" on page 12-119.)

To restrict Telnet access to all of the configuration screens, select **Enable Telnet Console Access** and toggle it to **No**.

About filters and filter sets

Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network's security.

The Netopia R910's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the router's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called firewalling your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What's a filter and what's a filter set?

A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can be either an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

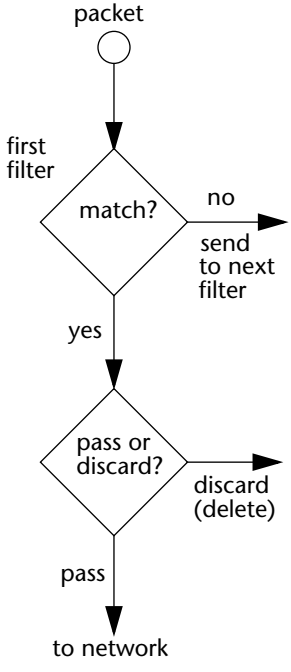
A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to see if it matches that destination.

A filter inspects data packets like a customs inspector scrutinizing packages.

Filter priority

Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.



If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can pass or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither pass nor discard the packet (because it cannot match any criteria), the second filter has a chance to pass or reject it, and so on. Because of this hierarchical structure, each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

A filter's actions

- Passes the packet to the local or remote network
- Blocks (discards) the packet
- Ignores the packet

A filter passes or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

A filtering rule

The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

Block all Telnet attempts that originate from the remote host 199.211.211.17.

This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.

Here is what this rule looks like when implemented as a filter on the Netopia R910:

```
+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------+
| 1  199.211.211.17  0.0.0.0          TCP   23               Yes No  |
+-------------------------------------------------------------------+
```

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

- The source IP address (where the packet was sent from)
- The destination IP address (where the packet is going)
- The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Port numbers

A filter can also match a packet's port number attributes, but only if the filter's protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

- The source port number (the port on the sending host that originated the packet)
- The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The tables below show a few common services and their associated port numbers.

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80
SMTP (mail)	25	News	144
Gopher	70	rlogin	513

Internet service	UDP port	Internet service	UDP port
Who Is	43	AppleTalk Routing Maintenance (at-rtmp)	202
World Wide Web	80	AppleTalk Name Binding (at-nbp)	202
SNMP	161	AURP (AppleTalk)	387
TFTP	69	who	513

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

No Compare: No comparison of the port number specified in the filter with the packet's port number.

Not Equal To: For the filter to match, the packet's port number cannot equal the port number specified in the filter.

Less Than: For the filter to match, the packet's port number must be less than the port number specified in the filter.

Less Than or Equal: For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.

Equal: For the filter to match, the packet's port number must equal the port number specified in the filter.

Greater Than: For the filter to match, the packet's port number must be greater than the port number specified in the filter.

Greater Than or Equal: For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

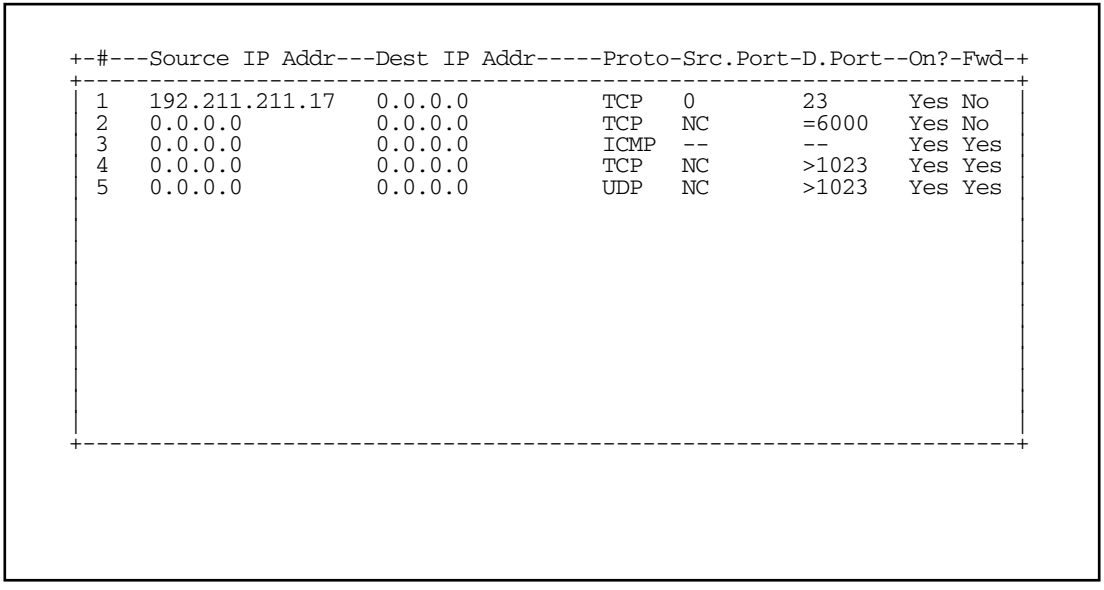
Other filter attributes

There are three other attributes to each filter:

- The filter's order (i.e., priority) in the filter set
- Whether the filter is currently active
- Whether the filter is set to pass (forward) packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:



#	Source IP Addr	Dest IP Addr	Proto	Src.Port	D.Port	On?	Fwd
1	192.211.211.17	0.0.0.0	TCP	0	23	Yes	No
2	0.0.0.0	0.0.0.0	TCP	NC	=6000	Yes	No
3	0.0.0.0	0.0.0.0	ICMP	--	--	Yes	Yes
4	0.0.0.0	0.0.0.0	TCP	NC	>1023	Yes	Yes
5	0.0.0.0	0.0.0.0	UDP	NC	>1023	Yes	Yes

The table's columns correspond to each filter's attributes:

#: The filter's priority in the set. Filter number 1, with the highest priority, is first in the table.

Source IP Addr: The packet source IP address to match.

Dest IP Addr: The packet destination IP address to match.

Proto: The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if those protocols are used.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

Src. Port: The source port to match. This is the port on the sending host that originated the packet.

D. Port: The destination port to match. This is the port on the receiving host for which the packet is intended.

On?: Displays **Yes** when the filter is in effect or **No** when it is not.

Fwd: Shows whether the filter forwards (**Yes**) a packet or discards (**No**) it when there's a match.

Filtering example #1

Returning to our filtering rule example from above (see page 13-128), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

1. The rule you want to implement as a filter is:

   Block all Telnet attempts that originate from the remote host 199.211.211.17.

2. The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Dest IP Addr could have been anything. The mask for Source IP Addr must be 255.255.255.255 since an exact match is desired.

   - Source IP Addr = 199.211.211.17
   - Source IP address mask = 255.255.255.255
   - Dest IP Addr = 0.0.0.0
   - Destination IP address mask = 0.0.0.0

   Note: To learn about IP addresses and masks, see Appendix B, "Understanding IP Addressing."

3. Using the tables on page 13-129, find the destination port and protocol numbers (the *local* Telnet port):

   - Proto = TCP (or 6)
   - D. Port = 23

4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:
   - On? = Yes
   - Fwd = No

This four-step process is how we produced the following filter from the original rule:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0          TCP   0        23       Yes No   |
|                                                                         |
+-------------------------------------------------------------------------+
```

Filtering example #2

Suppose a filter is configured to block all incoming IP packets with the source IP address of 200.233.14.0, regardless of the type of connection or its destination. The filter would look like this:

```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------------+
| 1   200.233.14.0     0.0.0.0               0                Yes No   |
|                                                                         |
+-------------------------------------------------------------------------+
```

This filter blocks any packets coming from a remote network with the IP network address 200.233.14.0. The 0 at the end of the address signifies *any* host on the class C IP network 200.233.14.0. If, for example, the filter is applied to a packet with the source IP address 200.233.14.5, it will block it.

In this case, the mask, which does not appear in the table, must be set to 255.255.255.0. This way, all packets with a source address of 200.233.14.x will be matched correctly, no matter what the final address byte is.

Note: The protocol attribute for this filter is 0 by default. This tells the filter to ignore the IP protocol or type of IP packet.

Design guidelines

Careful thought must go into designing a new filter set. You should consider the following guidelines:

- Be sure the filter set's overall purpose is clear from the beginning. A vague purpose can lead to a faulty set, and that can actually make your network *less* secure.
- Be sure each individual filter's purpose is clear.
- Determine how filter priority will affect the set's actions. Test the set (on paper) by determining how the filters would respond to a number of different hypothetical packets.
- Consider the combined effect of the filters. If every filter in a set fails to match on a particular packet, the packet is:
  - Passed if all the filters are configured to discard (*not* forward)

- Discarded if all the filters are configured to pass (forward)
- Discarded if the set contains a combination of pass and discard filters

Disadvantages of filters

Although using filter sets can greatly enhance network security, there are disadvantages:

- Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.
- Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints.
- Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, caller ID, the "must match" option in the answer profile, PAP or CHAP in connection profiles, callback, and general awareness of how your network may be vulnerable.

An approach to using filters

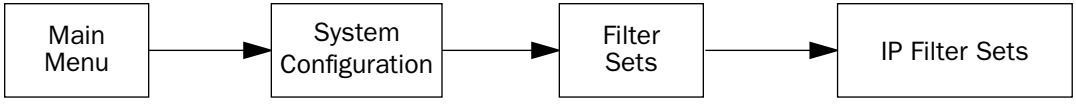
The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

Each filter set you design will be based on one of the following approaches:

- That which is not expressly prohibited is permitted.
- That which is not expressly permitted is prohibited.

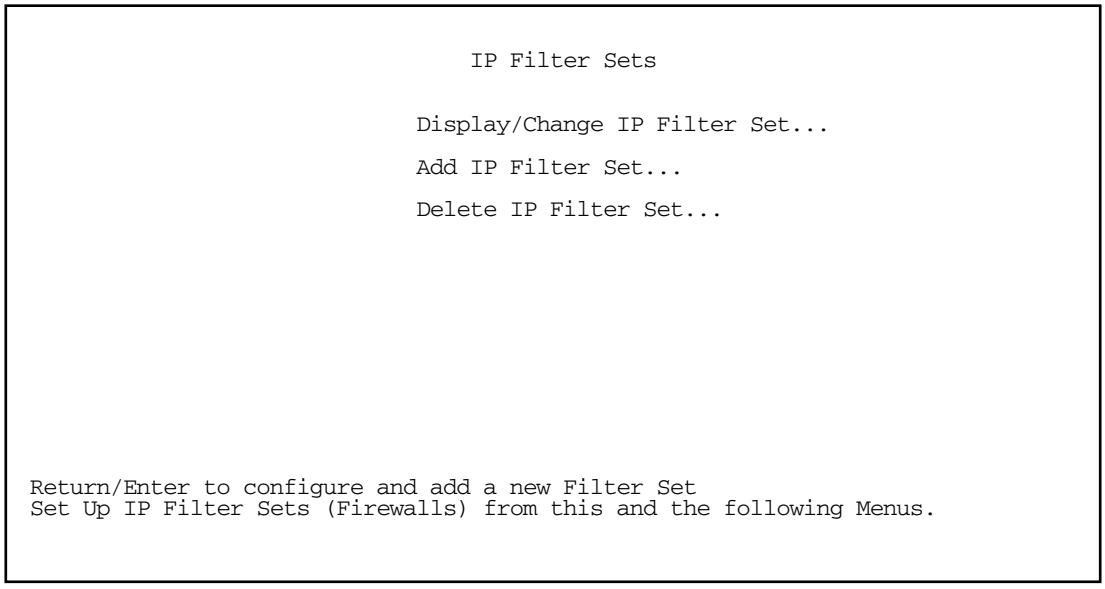
It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.

Working with IP filters and filter sets



To work with filters and filter sets, begin by accessing the filter set screens.

Note: Make sure you understand how filters work before attempting to use them. Read the section "About filters and filter sets," beginning on page 13-126.



The procedure for creating and maintaining filter sets is as follows:

1. Add a new filter set.
2. Create the filters for the new filter set.
3. View, change, or delete individual filters and filter sets.

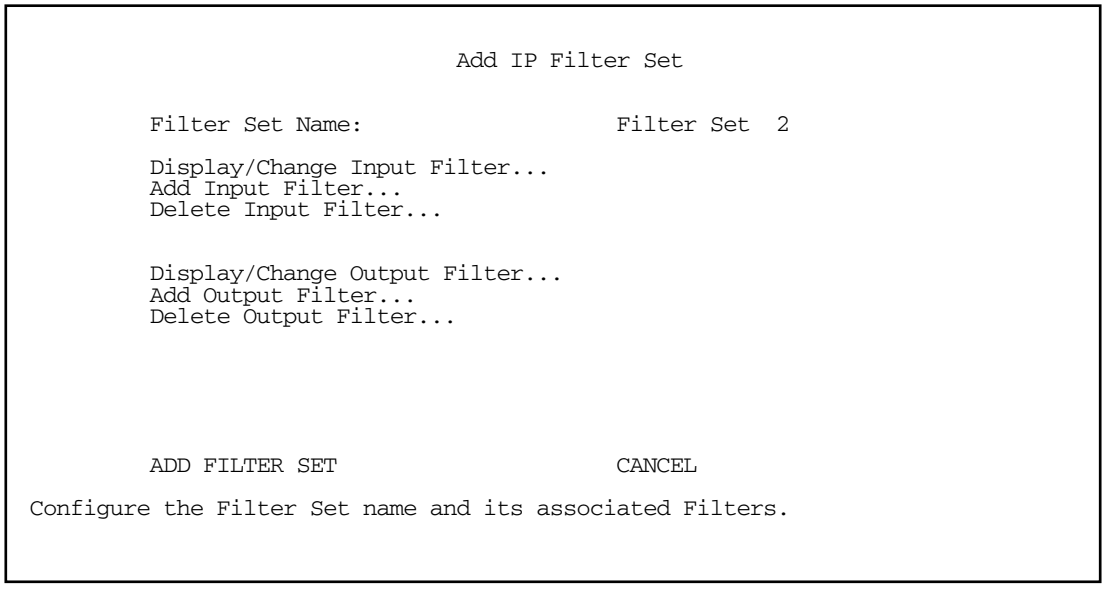
The sections below explain how to execute these steps.

Adding a filter set

You can create up to eight different custom filter sets. Each filter set can contain up to 16 output filters and up to 16 input filters.

To add a new filter set, select **Add IP Filter Set** in the IP Filter Sets screen and press Return. The Add Filter Set screen appears.

Note: There are two groups of items in the Add IP Filter Set screen, one for input filters and one for output filters. The two groups work in essentially the same way, as you'll see below.



Naming a new filter set

All new filter sets have a default name. The first filter set you add will be called Filter Set 1, the next filter will be Filter Set 2, and so on.

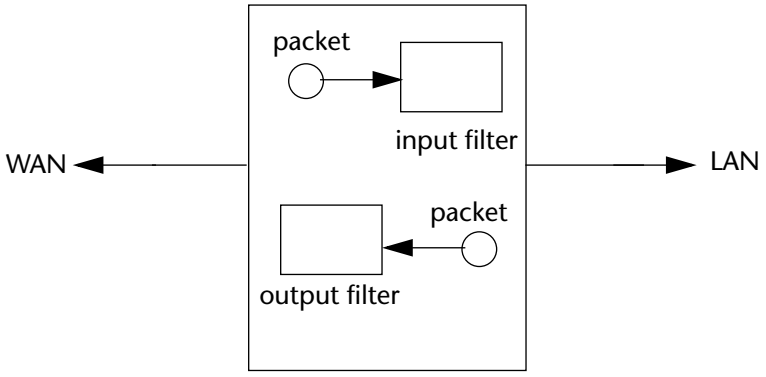
To give a new filter set a different name, select **Filter Set Name** and enter a new name for the filter set.

To save the filter set, select **ADD FILTER SET**. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see "Modifying filter sets" on page 13-139). Or you can add filters to your new set before saving it (see "Adding filters to a filter set" on page 13-136).

To leave the Add Filter Set screen without saving the new filter set Select **CANCEL**. You are returned to the IP Filter Sets screen.

Input and output filters—source and destination

There are two kinds of filters you can add to a filter set: input and output. Input filters check packets received from the Internet, destined for your network. Output filters check packets transmitted from your network to the Internet.



The Netopia R910 Router

Packets in the Netopia R910 pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

The process for adding input and output filters is exactly the same. The main difference between the two involves their reference to source and destination. From the perspective of an input filter, your local network is the **destination** of the packets it checks, and the remote network is their **source**. From the perspective of an output filter, your local network is the **source** of the packets, and the remote network is their **destination**.

Type of filter	"Source" means	"Destination" means
Input filter	The remote network	The local network
Output filter	The local network	The remote network

Adding filters to a filter set

In this section you'll learn how to add an input filter to a filter set. Adding an output filter works exactly the same way, providing you keep the different source and destination perspectives in mind.

To add an input filter, select **Add Input Filter** in the Add IP Filter Set screen. The Add Filter screen appears. (To add an output filter, select **Add Output Filter**.)

```
                                Add Filter

                        Enabled:                    No
                        Forward:                    No

                        Source IP Address:          0.0.0.0
                        Source IP Address Mask:     0.0.0.0

                        Dest. IP Address:           0.0.0.0
                        Dest. IP Address Mask:      0.0.0.0

                        Protocol Type:              0

                        Source Port Compare...      No Compare
                        Source Port ID:             0
                        Dest. Port Compare...       No Compare
                        Dest. Port ID:              0

                        ADD THIS FILTER NOW         CANCEL

Enter the IP specific information for this filter.
```

1. To make the filter active in the filter set, select **Enabled** and toggle it to **Yes**. If **Enabled** is toggled to **No**, the filter can still exist in the filter set, but it will have no effect.
2. If you want the filter to forward packets that match its criteria to the destination IP address, select **Forward** and toggle it to **Yes**. If **Forward** is toggled to **No**, packets matching the filter's criteria will be discarded.
3. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.
4. Select **Source IP Address Mask** and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.
5. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.
6. Select **Dest. IP Address Mask** and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.
7. Select **Protocol Type** and enter **ICMP**, **TCP**, **UDP**, **Any**, or the number of another IP transport protocol (see the table on page 13-131).

   Note: If Protocol Type is set to TCP or UDP, the settings for port comparison that you configure in steps 8 and 9 will appear. These settings only take effect if the Protocol Type is TCP or UDP.
8. Select **Source Port Compare** and choose a comparison method for the filter to use on a packet's source port number. Then select **Source Port ID** and enter the actual source port number to match on (see the table on page 13-129).
9. Select **Dest. Port Compare** and choose a comparison method for the filter to use on a packet's destination port number. Then select **Dest. Port ID** and enter the actual destination port number to match on (see the table on page 13-129).

10. When you are finished configuring the filter, select **ADD THIS FILTER NOW** to save the filter in the filter set. Select **CANCEL** to discard the filter and return to the Add IP Filter Set screen.

Viewing filters

To display a view-only table of input (output) filters, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Add IP Filter Set screen.

Modifying filters

To modify a filter, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Add IP Filter Set screen to display a table of filters.

Select a filter from the table and press Return. The Change Filter screen appears. The parameters in this screen are set in the same way as the ones in the Add Filter screen (see "Adding filters to a filter set" on page 13-136).

```
                                Change Filter

                        Enabled:                    No
                        Forward:                    No

                        Source IP Address:          0.0.0.0
                        Source IP Address Mask:     0.0.0.0

                        Dest. IP Address:           0.0.0.0
                        Dest. IP Address Mask:      0.0.0.0

                        Protocol Type:              0

                        Source Port Compare...      No Compare
                        Source Port ID:             0
                        Dest. Port Compare...       No Compare
                        Dest. Port ID:              0


Enter the IP specific information for this filter.
```

Deleting filters

To delete a filter, select **Delete Input Filter** or **Delete Output Filter** in the Add IP Filter Set screen to display a table of filters.

Select the filter from the table and press Return to delete it. Press Escape to exit the table without deleting the filter.

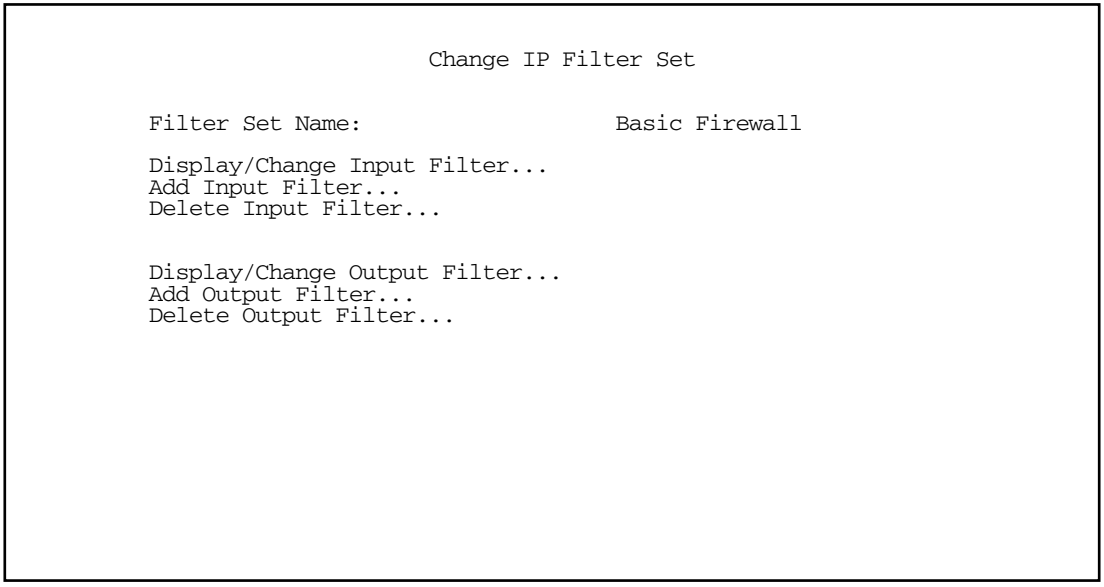
Viewing filter sets

To display a view-only list of filter sets, select **Display/Change IP Filter Set** in the IP Filter Sets screen.

Modifying filter sets

To modify a filter set, select **Display/Change IP Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return. The Change IP Filter Set screen appears. The items in this screen are the same as the ones in the Add Filter screen (see "Adding filters to a filter set" on page 13-136).



Deleting a filter set

Note: If you delete a filter set, all of the filters it contains are deleted as well. To reuse any of these filters in another set, before deleting the current filter set you'll have to note their configuration and then recreate them.

To delete a filter set, select **Delete IP Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to delete it. Press Escape to exit the list without deleting the filter set.

A sample IP filter set

This section contains the settings for a filter set called Basic Firewall, which is part of the Netopia R910's factory configuration.

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but passes all traffic originating from the LAN. It follows the conservative "that which is not expressly permitted is prohibited" approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall's filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect since filter 4 would have already passed OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly passes all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters pass all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter passes all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

Basic Firewall is suitable for a LAN containing only client hosts that want to access servers on the WAN, but not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly pass WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See the next section, "Possible modifications," for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if you are making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: e.f.g.h
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: 0.0.0.0
- Source IP Address Mask: 0.0.0.0
- Dest. IP Address: a.b.c.d
- Dest. IP Address Mask: 255.255.255.255
- Protocol Type: TCP
- Source Port Comparison: No Compare
- Source Port ID: 0
- Dest. Port Comparison: Equal
- Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or to 80 for WWW.

AURP tunnel. To allow an AURP tunnel between a remote AURP router with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243) and a local AURP router (including the Netopia R910 itself), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: UDP
- Source Port Comparison: Equal
- Source Port ID: 387
- Dest. Port Comparison: Equal
- Dest. Port ID: 387

Firewall tutorial

General firewall terms

Filter rule: A filter set is comprised of individual filter rules.

Filter set: A grouping of individual filter rules.

Firewall: A component or set of components that restrict access between a protected network and the Internet, or between two networks.

Host: A workstation on the network.

Packet: Unit of communication on the Internet.

Packet filter: Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports, or the TCP ACK bit.

Port: A number that defines a particular type of service.

Basic IP packet components

All IP packets contain the same basic header information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27
Source Port	2541
Destination Port	80
Protocol	TCP
ACK Bit	Yes
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that a packet filter does not look into the IP data stream (the User Data from above) to make filtering decisions.

Basic protocol types

TCP: Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.

UDP: User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not retransmit the data. RFC 768 is the specification for UDP.

There are many more ports defined in the Assigned Addresses RFC. The table that follows shows some of these port assignments.

Example TCP/UDP Ports

TCP Port	Service	UDP Port	Service
20/21	FTP	161	SNMP
23	Telnet	69	TFTP
25	SMTP	387	AURP
80	WWW		
144	News		

Firewall design rules

There are two basic rules to firewall design:

- "What is not explicitly allowed is denied."

and

- "What is not explicitly denied is allowed."

The first rule is far more secure, and is the best approach to firewall design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and in the future.

Firewall Logic

Firewall design is a test of logic, and filter rule ordering is critical. If a packet is passed through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not pass through the remainder of the filter rules.

For example, if you had the following filter set...

Allow WWW access;

Allow FTP access;

Allow SMTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first rule (WWW), go through the second rule (FTP), and match this rule; the packet is allowed through.

If you had this filter set for example....

Allow WWW access;

Allow FTP access;

Deny FTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first filter rule (WWW), match the second rule (FTP), and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Binary representation

It is easiest when doing filtering to convert the IP address and mask in question to binary. This will allow you to perform the logical AND to determine whether a packet matches a filter rule.

Logical AND function

When a packet is compared (in most cases) a logical AND function is performed. First the IP addresses and subnet masks are converted to binary and then combined with AND. The rules for the logical use of AND are as follows:

0 AND 0 = 0

0 AND 1 = 0

1 AND 0 = 0

1 AND 1 = 1

For example:

Filter rule:

Deny

IP: 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

Mask: 255.255.255.255 BINARY: 11111111.11111111.11111111.11111111

Incoming Packet:

IP 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

If you put the incoming packet and subnet mask together with AND, the result is:

10100011.10110000.00000001.00001111

which matches the IP address in the filter rule and the packet is denied.

Implied rules

With a given set of filter rules, there is an Implied rule that may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied rule is NO.
N+N+N=Y	If all filter rules are NO, the implied rule is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied rule is NO.

Established connections

The TCP header contains one bit called the ACK bit (or TCP Ack bit). This ACK bit appears only with TCP, not UDP. The ACK bit is part of the TCP mechanism that guaranteed the delivery of data. The ACK bit is set whenever one side of a connection has received data from the other side. Only the first TCP packet will not have the ACK bit set; once the TCP connection is in place, the remainder of the TCP packets with have the ACK bit set.

The ACK bit is helpful for firewall design and reduces the number of potential filter rules. A filter rule could be created just allowing incoming TCP packets with the ACK bit set, since these packets had to be originated from the local network.

Example IP filter set screen

This is an example of the Netopia IP filter set screen:

```
                              Change Filter

          Enabled:                          Yes
          Forward:                          No

          Source IP Address:                0.0.0.0
          Source IP Address Mask:           0.0.0.0

          Dest. IP Address:                 0.0.0.0
          Dest. IP Address Mask:            0.0.0.0

          Protocol Type:                    TCP

          Source Port Compare...            No Compare
          Source Port ID:                   0
          Dest. Port Compare...             Equal
          Dest. Port ID:                    2000
          Established TCP Conns. Only:      No


Return/Enter accepts * Tab toggles * ESC cancels.
Enter the IP specific information for this filter.
```

Filter basics

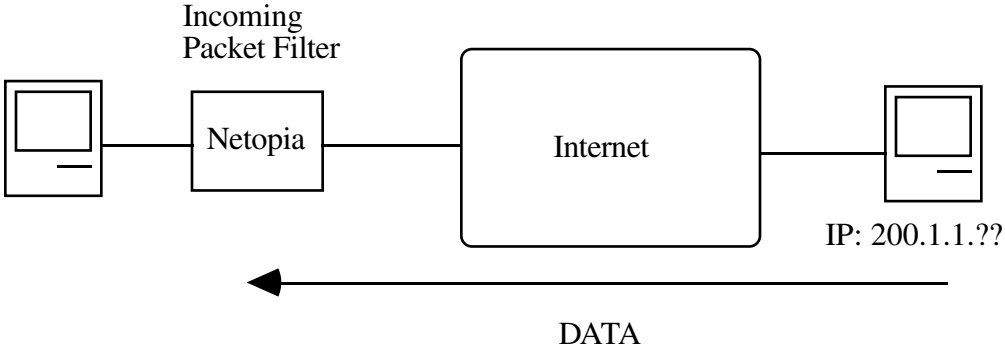
In the source or destination IP address fields, the IP address that is entered must be the network address of the subnet. A host address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

The Netopia R910 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No Compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined

Less Than or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined

Example network



Example filters

Example 1

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

IP Address	Binary Representation	
200.1.1.28	00011100	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	00000000	(Logical AND result)

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field (00000000) in the Netopia R910. This will *not* forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	10000000	(Logical AND result)

This incoming IP packet (10000000) has a source IP address that does not match the network address in the Source IP Address field (00000000) in the Netopia R910. This rule *will* forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	10110000	(Logical AND result)

Since the Source IP Network Address in the Netopia R910 is 01100000, and the source IP address after the logical AND is 1011000, this rule does *not* match and this packet will be passed.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104.

IP Address	Binary Representation	
200.1.1.104	01101000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R910 is 01100000, and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will *not* be passed.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96.

IP Address	Binary Representation	
200.1.1.96	01100000	(Source address in incoming IP packet)
AND		
255.255.255.255	11111111	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia R910 is 01100000, and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will NOT be passed. This rule masks off a *single* IP address.

RADIUS Client Support

TheNetopia R910 implements a Remote Authentication Dial-In User Service (RADIUS) client (RFC 2138) and adds the ability to authenticate console configuration access using a RADIUS server. This feature is strictly for console menu access authentication only, and is not intended for WAN connectivity access authentication.

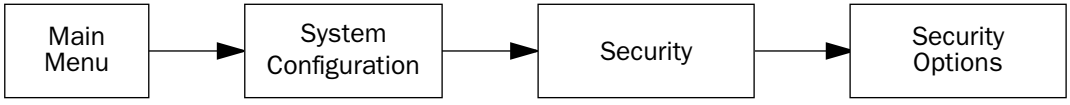
Earlier routers use a local console authentication database consisting of between one and four user-name/password pairs. They require a user seeking console configuration access to log in with a username and password when at least one username/password pair have been configured locally in the router. If no user-name/password pairs are defined, a user seeking console configuration access is given access without being required to log in.

TheR910 adds the ability to authenticate users seeking console configuration access by using a remote authentication database maintained by a RADIUS server. It supports four security database modes:

- Local Only
- RADIUS only
- RADIUS then Local
- Local then RADIUS

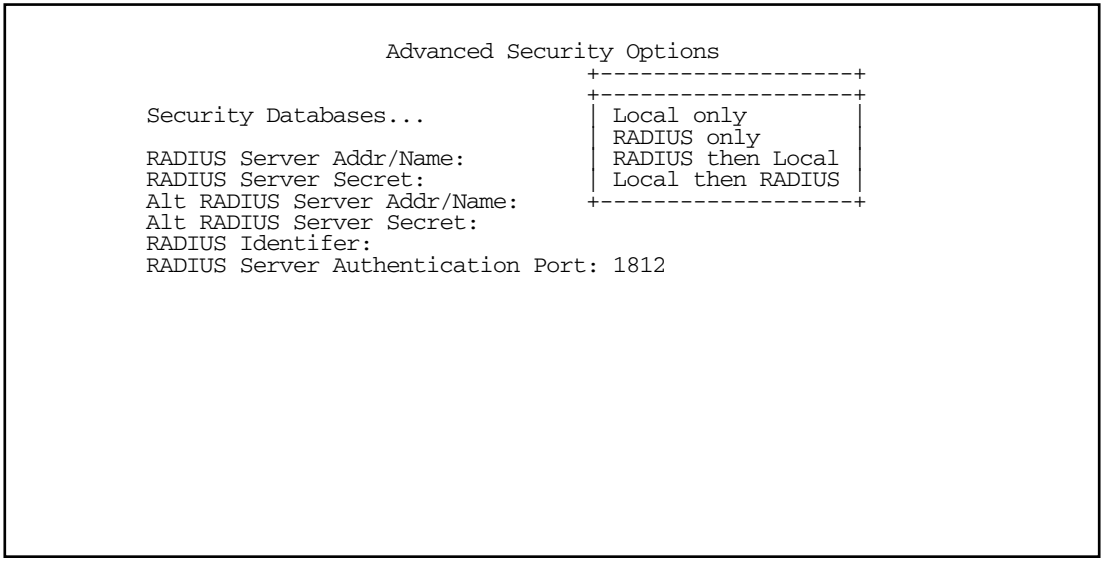
RADIUS client configuration

To display the Security Options screen, from the Main Menu select System Configuration, Security, then Security Options.




```
                          Security Options

        Enable Dial-in Console Access:                    Yes

        Enable SmartStart/Web Server:                     Yes

        Enable Telnet Console Access:                     Yes
        Enable Telnet Access to SNMP Screens:             Yes
        Console Access timeout (seconds):                 600

        Show Users...
        Add User...
        Delete User...

        Advanced Security Options...

        Password for This Screen (11 chars max):


Set up configuration access options here.
```

If you select **Advanced Security Options** and press Return, the Advanced Security Options screen appears.



- You select your desired mode by using the **Security Databases...** pop-up menu.
  - Choosing **Local Only**, the default, selects the standard authentication mechanism.
  - Choosing **RADIUS Only** causes the router to ignore the local database and to authenticate users using the configured RADIUS server.
  - Choosing **RADIUS then Local** causes the router to attempt to authenticate a user first using a RADIUS server and then, if that fails, using the local authentication database.
  - Choosing **Local then RADIUS** causes the router to attempt to authenticate a user first using the local authentication database, and then, if that fails using the configured RADIUS server.

Note: In the latter two modes that involve both RADIUS and the local database, if the local database includes no username/password pairs, authentication will succeed only if the RADIUS server authenticates the user. This differs from the Local Only mode where no authentication is performed when the local database is empty.

The alternate RADIUS server is not contacted if the primary RADIUS server responds, but responds with an Access-Reject or Access-Challenge response, only if the primary server fails to respond at all.

Therefore, do not attempt to select any of the RADIUS options unless you have a RADIUS server correctly configured for this purpose. If you attempt to use RADIUS authentication without a RADIUS server, you will lose your communication with the router.

The Advanced Security Options screen supports both a primary RADIUS server and an alternate RADIUS server. When the router is configured to authenticate using RADIUS, it will first attempt to contact the primary RADIUS server; if the primary RADIUS server responds, RADIUS authentication succeeds or fails based on the response returned by the primary server. If and only if the primary server fails to respond, the router will attempt to contact the alternate RADIUS server to authenticate the user. The router makes two attempts per server, three seconds apart.

- You can specify the **RADIUS Server Addr/Name** and the **Alt RADIUS Server Addr/Name** either by using a

hostname to be resolved using the Domain Name System (DNS) information configured in the router, or by using an IP address in dotted-quad notation. The RADIUS Server Addr/Name items are limited to 63 characters.

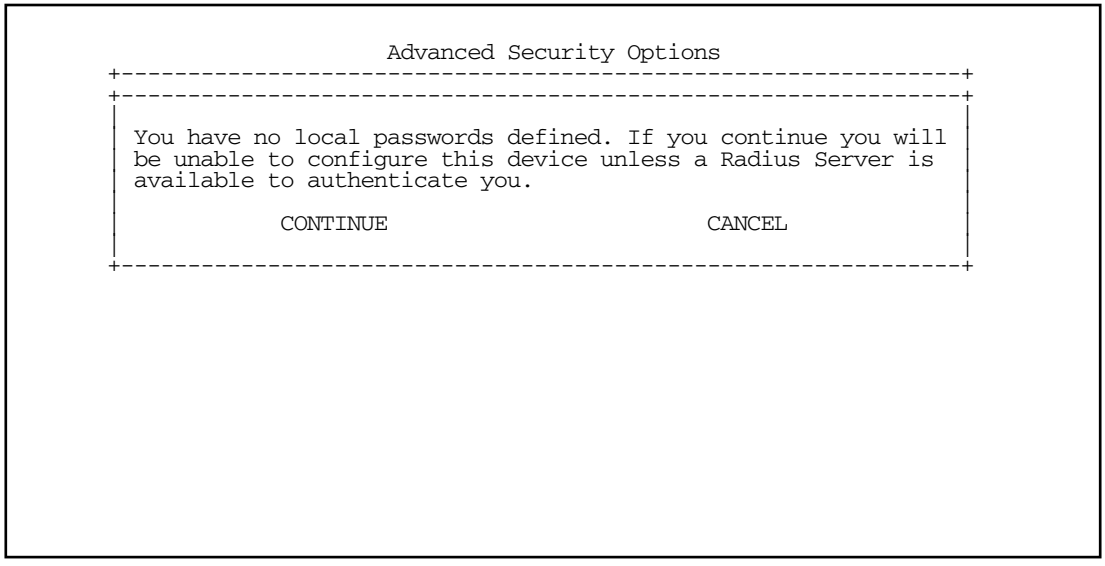
- In addition to specifying the server's hostname or IP address, you must also specify a **RADIUS Server Secret** and an **Alt RADIUS Server Secret** (if configured) known to both the router and the RADIUS server. The secret is used to encrypt RADIUS transactions in transit. The RADIUS Server Secret items are limited to 31 characters.

  The router's RADIUS client implementation supports passwords longer than 16 characters and properly encrypts such passwords per RFC 2138. Not all RADIUS server implementations handle passwords longer than 16 characters.

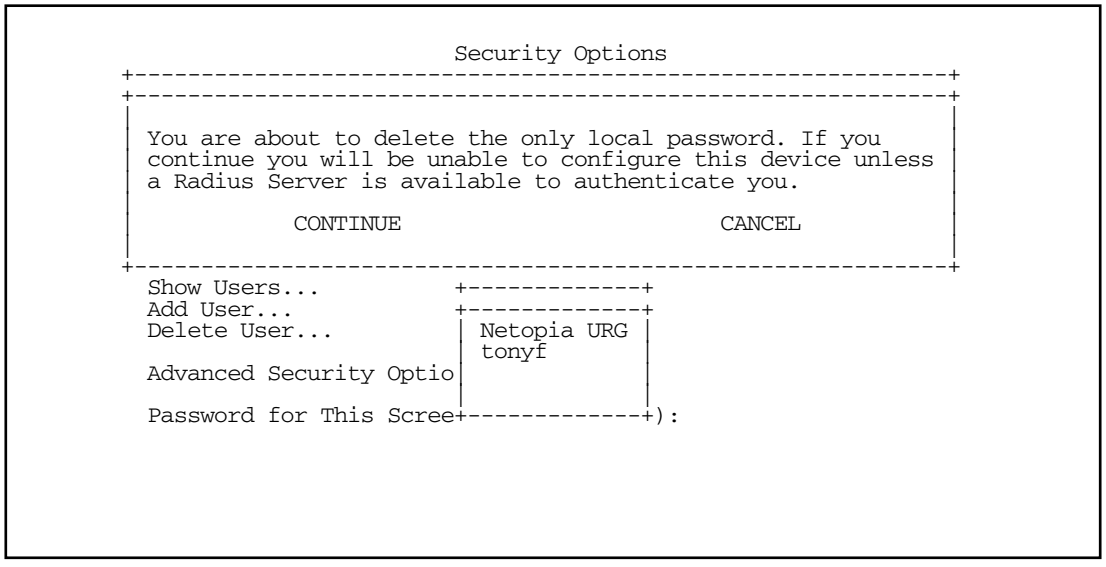
- **RADIUS Identifier** can be either an IP address or an arbitrary string to be used as the identifier in the router's outgoing Access-Request packets. The RADIUS identifier is limited to 63 characters.

- **RADIUS Server Authentication Port** specifies the UDP destination port to which the router's RADIUS authentication requests will be sent. The default value is 1812, the official IANA assigned UDP port number for the RADIUS authentication service.

Note: Certain security-related configuration changes cause the router to display a warning alert. Choosing either **Local then RADIUS** or **RADIUS then Local** from the Security Databases pop-up menu when there are no configured username/password pairs causes the router to present the following warning alert:



Attempting to delete the last non-URG username/password pair from the local authentication database when the Security Databases pop-up menu is set to either "Local then RADIUS" or "RADIUS then Local" causes the router to present the following warning alert:


Security Options
You are about to delete the only local password. If you
continue you will be unable to configure this device unless
a Radius Server is available to authenticate you.
CONTINUE
CANCEL
Show Users...
Add User...
Delete User...
Advanced Security Optio
Password for This Scree
Netopia URG
tonyf

Chapter 14

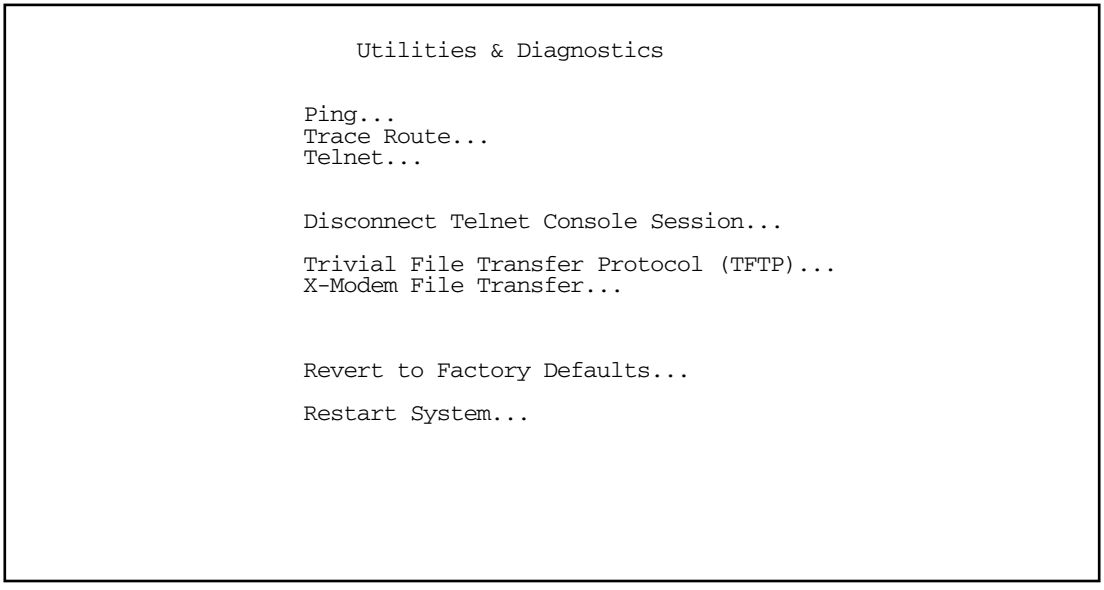
Utilities and Diagnostics

A number of utilities and tests are available for system diagnostic and control purposes.

This section covers the following topics:

Note: These utilities and tests are accessible only through the console-based management screens. See Chapter 6, "Console-Based Management," for information on accessing the console-based management screens.

You access the **Utilities & Diagnostics** screens from the **Main Menu**.

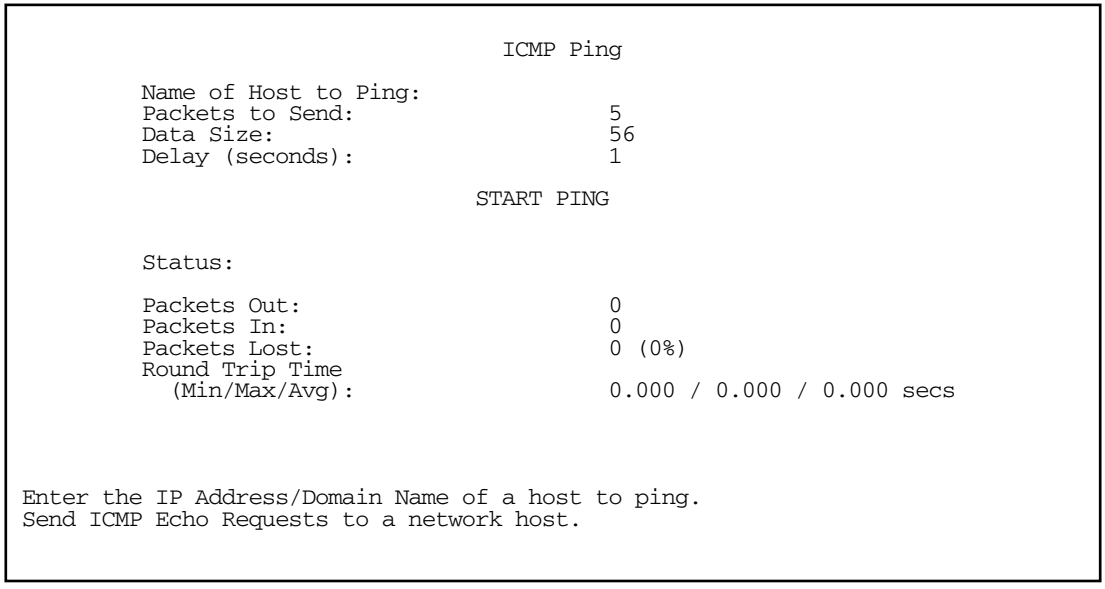


Ping

The Netopia R910 includes a standard Ping test utility. A Ping test generates IP packets destined for a particular (Ping-capable) IP host. Each time the target host receives a Ping packet, it returns a packet to the original sender.

Ping allows you to see whether a particular IP destination is reachable from the Netopia R910. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

In the Utilities & Diagnostic screen, select **Ping** and press Return. The ICMP Ping screen appears.



To configure and initiate a Ping test, follow these steps:

1. Select **Name of Host to Ping** and enter the destination domain name or IP address.
2. Select **Packets to Send** to change the default setting. This is the total number of packets to be sent during the Ping test. The default setting is adequate in most cases, but you can change it to any value from 1 to 4,294,967,295.
3. Select **Data Size** to change the default setting. This is the size, in bytes, of each Ping packet sent. The default setting is adequate in most cases, but you can change it to any value from 0 (only header data) to 1664.
4. Select **Delay (seconds)** to change the default setting. The delay, in seconds, determines the time between Ping packets sent. The default setting is adequate in most cases, but you can change it to any value from 0 to 4,294,967. A delay of 0 seconds forces packets to be sent immediately, one after another.
5. Select **START PING** and press Return to begin the Ping test. While the test is running, the **START PING** item becomes **STOP PING**. To manually stop the Ping test, select **STOP PING** and press Return or Escape.

While the Ping test is running and when it is over, a status field and a number of statistical items are active on the screen. These are described below.

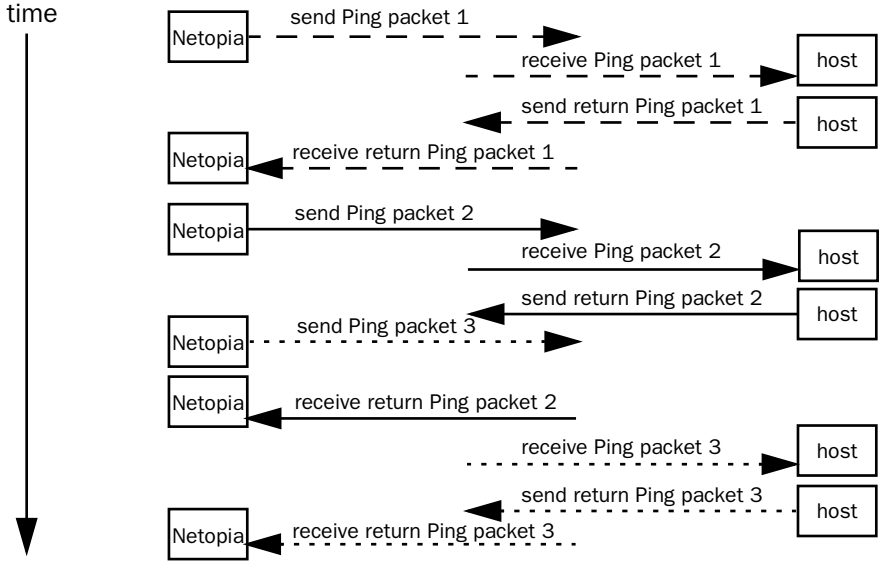
Status: The current status of the Ping test. This item can display the status messages shown in the able below:

Message	Description
Resolving host name	Finding the IP address for the domain name-style address
Can't resolve host name	IP address can't be found for the domain name–style name
Pinging	Ping test is in progress
Complete	Ping test was completed
Cancelled by user	Ping test was cancelled manually
Destination unreachable from w.x.y.z	Ping test was able to reach the router with IP address w.x.y.z, which reported that the test could not reach the final destination
Couldn't allocate packet buffer	Couldn't proceed with Ping test; try again or reset system
Couldn't open ICMP port	Couldn't proceed with Ping test; try again or reset system

Packets Out: The number of packets sent by the Ping test.

Packets In: The number of return packets received from the target host. To be considered "on time," return packets are expected back before the next packet in the sequence of Ping packets is sent. A count of the number of late packets appears in parentheses to the right of the **Packets In** count.

In the example that follows, a Netopia R910 is sending Ping packets to another host, which responds with return Ping packets. Note that the second return Ping packet is considered to be late because it is not received by the Netopia R910 before the third Ping packet is sent. The first and third return Ping packets are on time.



Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between **Packets Out** and **Packets Lost**, and **Packets In** is noticeably lagging behind **Packets Out**, the destination is probably unreachable. In this case, use **STOP PING**.

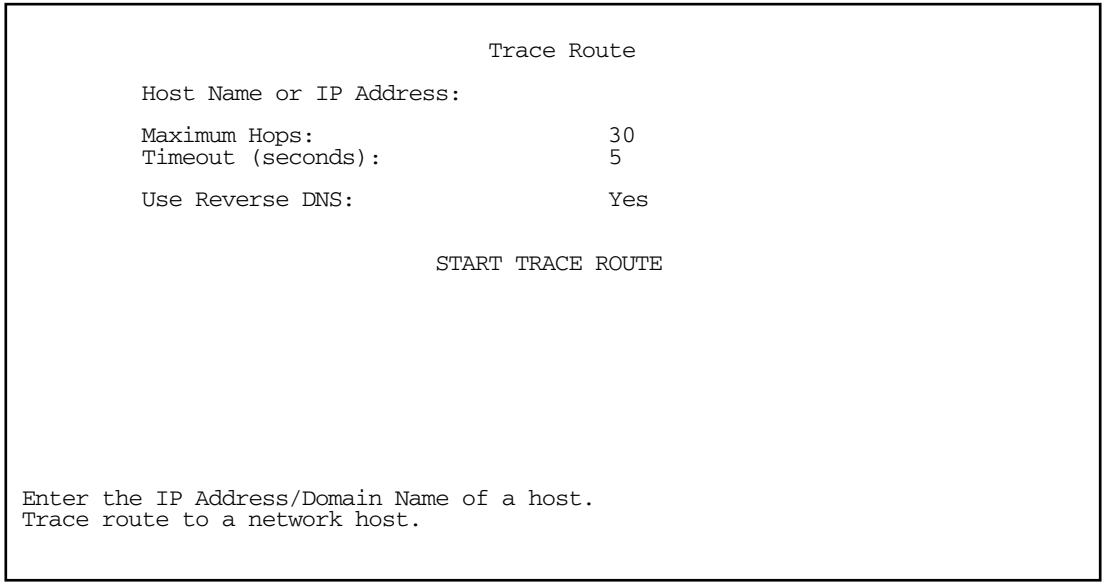
Round Trip Time (Min/Max/Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Netopia R910 is 255, the maximum allowed. The TTL value defines the number of IP routers that the packet can traverse. Ping packets that reach their TTL value are dropped, and a "destination unreachable" notification is returned to the sender (see the table on the previous page). This ensures that no infinite routing loops occur. The TTL value can be set and retrieved using the SNMP MIB-II ip group's ipDefaultTTL object.

Trace Route

You can count the number of routers between your Netopia Router and a given destination with the Trace Route utility.

In the Statistics & Diagnostics screen, select **Trace Route** and press Return. The Trace Route screen appears.



To trace a route, follow these steps:

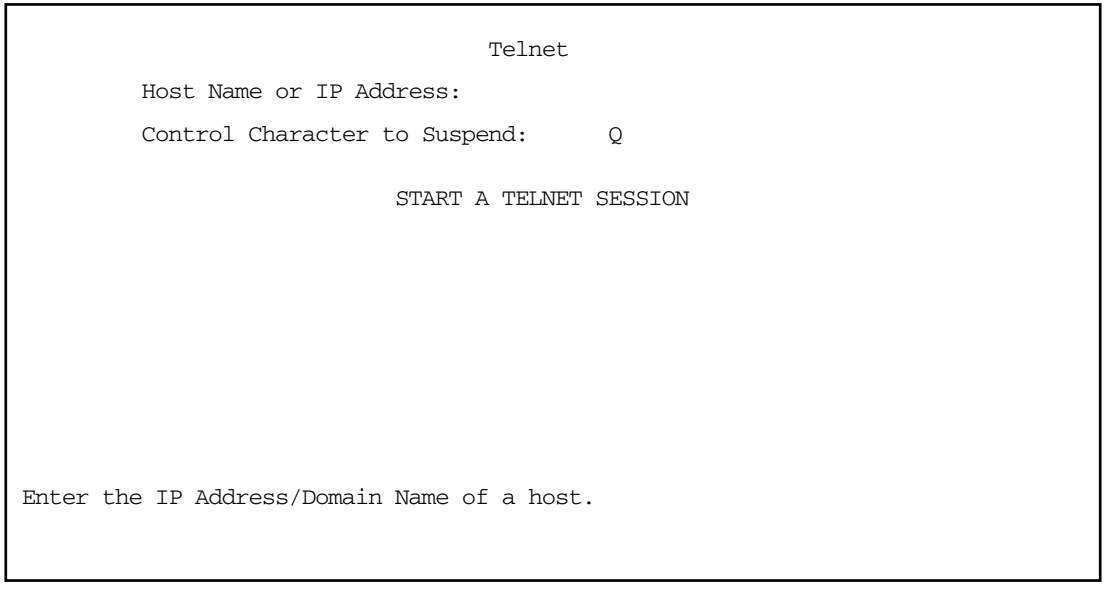
1. Select **Host Name or IP Address** and enter the name or address of the destination you want to trace.
2. Select **Maximum Hops** to set the maximum number of routers to count between the Netopia Router and the destination router, up to the maximum of 64. The default is 30 hops.
3. Select **Timeout (seconds)** to set when the trace will timeout for each hop, up to 10 seconds. The default is 3 seconds.

4. Select **Use Reverse DNS** to learn the names of the routers between the Netopia Router and the destination router. The default is Yes.
5. Select **START TRACE ROUTE** and press Return. A scrolling screen will appear that lists the destination, number of hops, IP addresses of each hop, and DNS names, if selected.
6. Cancel the trace by pressing Escape. Return to the Trace Route screen by pressing Escape twice.

Telnet client

The Telnet client mode replaces the normal menu mode. Telnet sessions can be cascaded, that is, you can initiate a Telnet client session when using a Telnet console session. To activate the Telnet client, select **Telnet** from the Utilities & Diagnostics menu.

The Telnet client screen appears.



- Enter the host name or the IP address in dotted decimal format of the machine you want to telnet into and press Return.
- Either accept the default control character “Q” used to suspend the Telnet session, or type a different one.
- **START A TELNET SESSION** becomes highlighted.
- Press Return and the Telnet session will be initiated.
- To suspend the session, press Control-Q, or whatever other control character you specified.

  Two new options will appear in the Telnet screen (not shown):

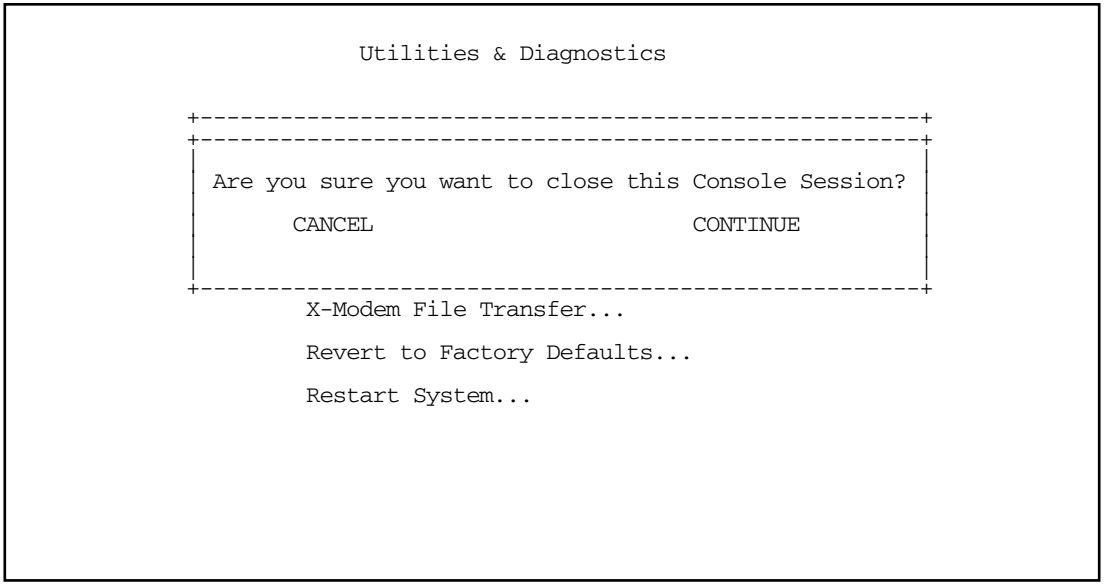
  Resume Suspended Session – select this one if you want to go back to your Telnet session

  Terminate Suspended Session – select this one if you want to end the session

Disconnect Telnet console session

If you want to close your Telnet Console session, select **Disconnect Telnet Console Session** and press Return.

A dialog box appears asking you to cancel or continue your selection.



If you select **Continue**, you will immediately terminate your session.

Factory defaults

You can reset the Netopia R910 to its factory default settings. In the Statistics & Diagnostics screen, select **Revert to Factory Defaults** and press Return. Select **CONTINUE** in the dialog box and press Return. The Netopia R910 will reboot and its settings will return to the factory defaults, deleting your configurations.

In an emergency, you can also use the Reset switch to return the router to its factory default settings. Call Netopia Tech Support for instructions on using the Reset switch.

Note: Reset to factory defaults with caution. You will need to reconfigure all of your settings in the router.

Transferring configuration and firmware files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the router as the client. To use the Netopia R910 as a TFTP client, a TFTP server must be available. Netopia, Inc. has a public access TFTP server on the Internet where you can obtain the latest firmware versions.

To use TFTP, select **Trivial File Transfer Protocol (TFTP)** in the Statistics & Diagnostics screen and press Return. The Trivial File Transfer Protocol (TFTP) screen appears.

```
                Trivial File Transfer Protocol (TFTP)

        TFTP Server Name:


        Firmware File Name:

        GET ROUTER FIRMWARE FROM SERVER...
        GET WAN MODULE FIRMWARE FROM SERVER...


        Config File Name:

        GET CONFIG FROM SERVER...
        SEND CONFIG TO SERVER...


        TFTP Transfer State -- Idle

        TFTP Current Transfer Bytes -- 0
```

The sections below describe how to update the Netopia R910's firmware and how to download and upload configuration files.

Updating firmware

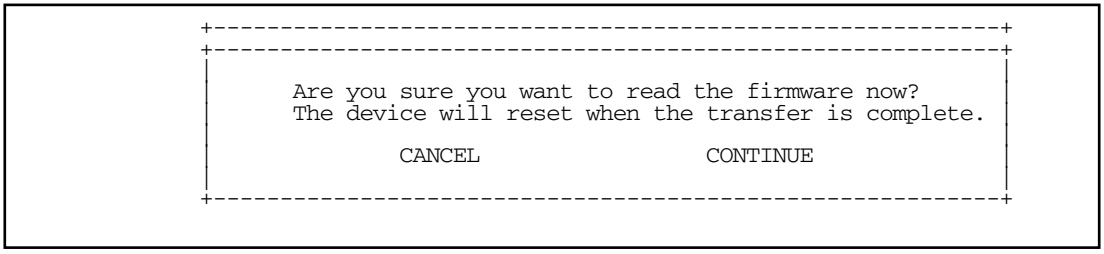
Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administrator.

There are two types of firmware in the Netopia R910 Ethernet Router: router firmware and WAN module firmware. The router firmware governs how the router communicates with your network and the WAN module; the WAN module firmware governs how the WAN module communicates with the remote site. WAN module firmware is included on your Netopia CD for XMODEM transfer and later updates will be available on the Netopia website. Router firmware updates are also periodically posted on the Netopia website.

To update either the router's or the internal WAN module's firmware, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Firmware File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).
- Select **GET ROUTER FIRMWARE FROM SERVER** or **GET WAN MODULE FIRMWARE FROM SERVER** and

press Return. You will see the following dialog box:



- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

- Be sure the firmware update you load onto your router is the correct version for your particular model. Some models do not support all firmware versions. Loading an incorrect firmware version can permanently damage the unit.
- Do not manually power down or reset the Netopia R910 while it is automatically resetting or it could be damaged.
- If you choose to download the firmware, the **TFTP Transfer State** item will change from **Idle** to **Reading Firmware**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

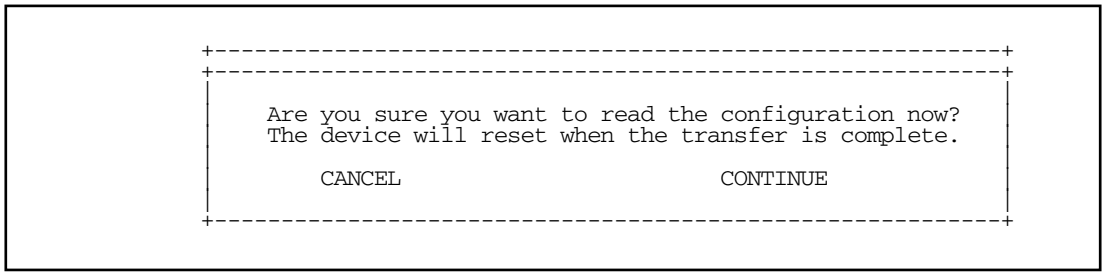
Downloading configuration files

The Netopia R910 can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the router's parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Config File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).

- Select **GET CONFIG FROM SERVER** and press Return. You will see the following dialog box:



- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new configuration into effect.
- If you choose to download the configuration file, the **TFTP Transfer State** item will change from **Idle** to **Reading Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Uploading configuration files

Using TFTP, you can send a file containing a snapshot of the router's current configuration to a TFTP server. The file can then be downloaded by a different Netopia R910 unit to configure its parameters (see "Downloading configuration files" on page 14-162). This is useful for configuring a number of routers with identical parameters, or just for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R910 unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
2. Select **Config File Name** and enter a name for the file you will upload. The file will appear with the name you choose on the TFTP server. You may need to enter a file path along with the file name (for example, Mypc/Netopia/myfile).
3. Select **SEND CONFIG TO SERVER** and press Return. Netopia will begin to transfer the file.
4. The **TFTP Transfer State** item will change from **Idle** to **Writing Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Transferring configuration and firmware files with XMODEM

You can transfer configuration and firmware files with XMODEM through the Netopia R910's console port. Be sure your terminal emulation program supports XMODEM file transfers.

To go to the **X-Modem File Transfer** screen, select it in the Utilities & Diagnostics menu.

Note: The X-Modem File Transfer screen is only available if you are connected via the Console port.

```
                    X-Modem File Transfer

        Send Firmware to Netopia...

        Send Config to Netopia...

        Receive Config from Netopia...


        Send Firmware to Netopia WAN module...

        WAN module Firmware Status:              IDLE
```

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administration. The procedure below applies whether you are using the console or the WAN interface module.

Follow these steps to update the Netopia R910's firmware:

1. Make sure you have the firmware file on disk and know the path to its location.
2. Select **Send Firmware to Netopia** (or **Send Firmware to Netopia WAN module**) and press Return. The following dialog box appears:

```
+-----------------------------------------------------------------+
+-----------------------------------------------------------------+
| Are you sure you want to send a firmware file to your Netopia?  |
| If so, when you hit Return/Enter on the CONTINUE button, you will |
| have 10 seconds to begin the transfer from your terminal program. |
|                                                                 |
|            CANCEL                        CONTINUE               |
|                                                                 |
|                                                                 |
+-----------------------------------------------------------------+
```

3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

   If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the firmware file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

The system will reset at the end of a successful file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

Do not manually power down or reset the Netopia R910 while it is automatically resetting or it could be damaged.

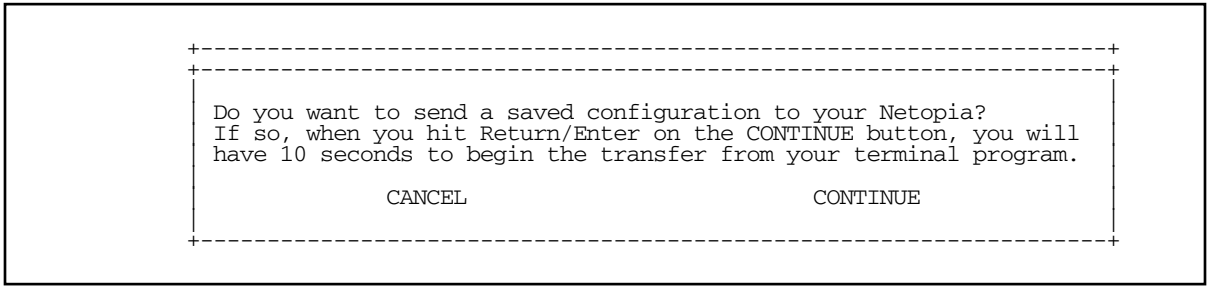
Downloading configuration files

The Netopia R910 can be configured by downloading a configuration file. The downloaded file reconfigures all of the Router's parameters.

Configuration files are available from a site maintained by your organization's network administrator or from your local site (see "Uploading configuration files," below).

Follow these steps to download a configuration file:

1. Make sure you have the configuration file on disk and know the path to its location.
2. Select **Send Config to Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

   If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

   The system will reset at the end of a successful file transfer to put the new configuration into effect.

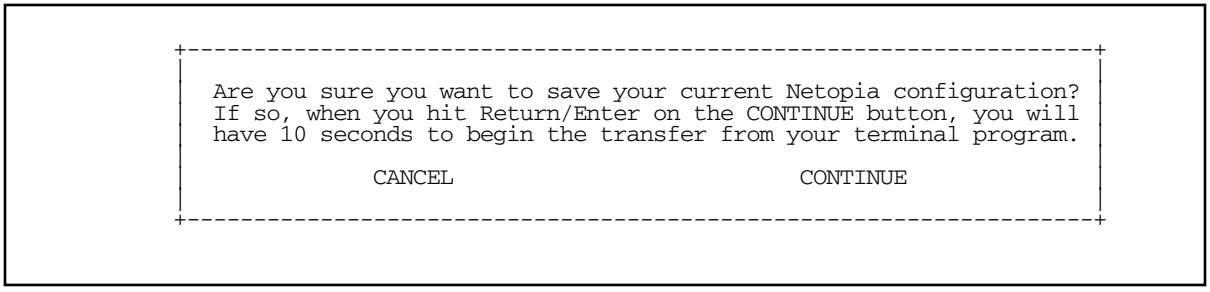
Uploading configuration files

A file containing a snapshot of the Netopia R910's current configuration can be uploaded from the router to disk. The file can then be downloaded by a different Netopia R910 to configure its parameters (see "Downloading configuration files," above). This is useful for configuring a number of routers with identical parameters or for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia R910 by Netopia or your network administrator.

The procedure below applies whether you are using the console or the WAN interface. To upload a configuration file:

1. Decide on a name for the file and a path for saving it.
2. Select **Receive Config from Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without uploading the file, or select **CONTINUE** to upload the file.

   If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

Restarting the system

You can restart the system by selecting the **Restart System** item in the Utilities & Diagnostics screen.

You must restart the system whenever you reconfigure the Netopia R910 and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions. Some configuration processes automatically restart the system to apply the changes you have made.

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while setting up and using the Netopia R910. It also includes information on how to contact Netopia Technical Support.

Important information on these problems can be found in the event histories kept by the Netopia R910. These event histories can be accessed in the Statistics & Logs screen.

This section covers the following topics:

Configuration problems

If you encounter problems during your initial configuration process, review the following suggestions before calling for technical support. There are four zones to consider when troubleshooting initial configuration:

1. The computer's connection to the router
2. The router's connection to the telecommunication line(s)
3. The telecommunication line's connection to your ISP
4. The ISP's connection to the Internet

If the connection from the computer to the router was not successful, verify that the following conditions are in effect:

- The Netopia R910 is turned on.
- An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Netopia R910.
- Telnet is available on your PC or Macintosh. (On a PC, it must be specified in your system path. You can usually find the application as "c:\windows\telnet.exe".)
- Your PC or Macintosh is properly configured for TCP/IP.
- Your PC or Macintosh has an IP address.
- Your PC or Macintosh has a subnet mask that matches or is compatible with the Netopia R910's subnet mask.

Note: If you are attempting to modify the IP address or subnet mask from a previous, successful configuration attempt, you will need to clear the IP address or reset your Netopia R910 to the factory default before reinitiating the configuration process. For further information on resetting your Netopia R910 to factory default, see "Factory defaults" on page 14-160.

Console connection problems

Can't see the configuration screens (nothing appears)

- Make sure the cable connection from the Netopia R910's console port to the computer being used as a console is securely connected.
- Make sure the terminal emulation software is accessing the correct port on the computer that's being used as a console.
- Try pressing Ctrl-L or Return or the ▲ up or down▼ key several times to refresh the terminal screen.
- Make sure that flow control on serial connections is turned off.

Junk characters appear on the screen

- Check that the terminal emulation software is configured correctly.
- Check the baud rate. The default values are 9600, N, 8, and 1.

Characters are missing from some of the configuration screens

- Try changing the Netopia R910's default speed of 9600 bps and setting your terminal emulation software to match the new speed.

Network problems

This section contains tips for troubleshooting a networking problem.

Problems communicating with remote IP hosts

- Verify the accuracy of the default gateway's IP address (entered in the IP Setup or Easy Setup screen).
- Use the Netopia R910's Ping utility, in the Utilities & Diagnostics screen, and try to ping local and remote hosts. See "Ping" on page 14-156 for instructions on how to use the Ping utility. If you can successfully ping hosts using their IP addresses but not their domain names (198.34.7.1 but not garcia.netopia.com, for example), verify that the DNS server's IP address is correct and that it is reachable from the Netopia R910 (use Ping).
- If you are using filters, check that your filter sets are not blocking the type of connections you are trying to make.

Local routing problems

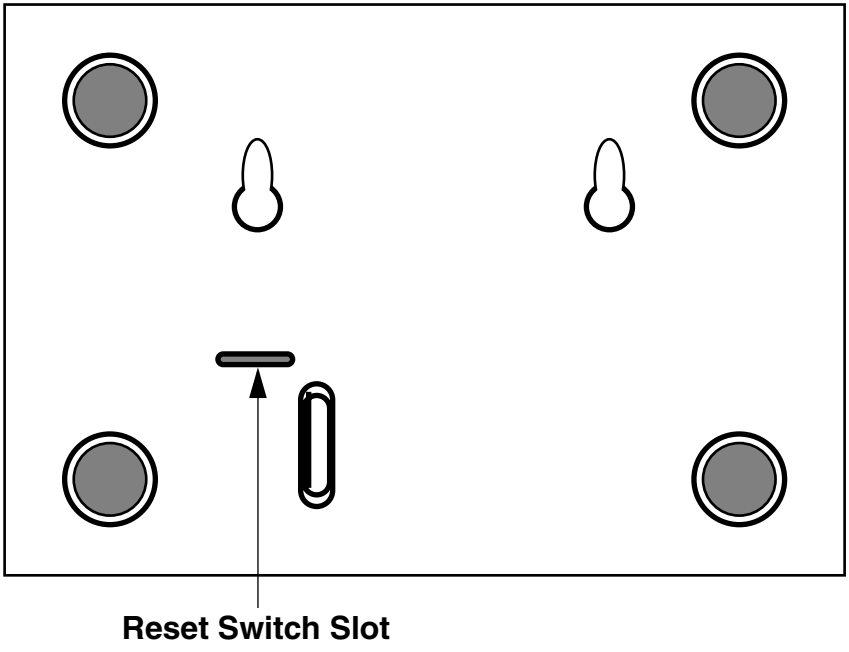
- Observe the Ethernet LEDs to see if data traffic flow appears to be normal.
- Check the WAN statistics and LAN statistics screens to see more specific information on data traffic flow and address serving. See "Statistics & Logs" on page 12-111 for more information.

How to reset the router to factory defaults

Lose your password? This section shows how to reset the router so that you can access the console screens once again. Keep in mind that all of your connection profiles and settings will need to be reconfigured.

If you don't have a password, the only way to get back into the Netopia R910 is the following:

1. Turn the router upside down.
2. Referring to the diagram below, find the paper clip size Reset Switch slot.



3. Carefully insert the larger end of a standard size paper clip until you contact the internal Reset Switch. (No need to unwind the paper clip.)
4. Press this switch.
5. This will reset the unit to factory defaults and you will now be able to reprogram the router.

Power outages

If you suspect that power was restored after a power outage and the Netopia R910 is connected to a remote site, you may need to switch the Netopia R910 off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the router should reestablish the connection.

Technical support

Netopia, Inc. is committed to providing its customers with reliable products and documentation, backed by excellent technical support.

Before contacting Netopia

Look in this guide for a solution to your problem. You may find a solution in this troubleshooting appendix or in other sections. Check the index for a reference to the topic of concern. If you cannot find a solution, complete the environment profile below before contacting Netopia technical support.

Environment profile

- Locate the Netopia R910's model number, product serial number, and firmware version. The serial number is on the bottom of the router, along with the model number. The firmware version appears in the Netopia R910's Main Menu screen.

  Model number:

  Serial number:

  Firmware version:

- What kind of local network(s) do you have, with how many devices?

  Ethernet

  LocalTalk

  EtherTalk

  TCP/IP

  Other:

How to reach us

We can help you with your problem more effectively if you have completed the environment profile in the previous section. If you contact us by telephone, please be ready to supply Netopia Technical Support with the information you used to configure the Netopia R910. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

When you are prepared, contact Netopia Customer Service by e-mail, telephone, fax, or post:

Internet: techsports@netopia.com (for technical support)
info@netopia.com (for general information)

Phone: 1 800-782-6449
Fax: 1 510-814-5023

Netopia, Inc.
Customer Service
2470 Mariner Square Loop
Alameda, California 94501
USA

Netopia Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Netopia World Wide Web server via http://www.netopia.com
Internet via anonymous FTP to ftp.netopia.com/pub

Online Technical Support

Technical notes and Frequently Asked Questions which answer the most commonly asked questions and offer solutions for many common problems are available 24 hours a day on our Company Web site at http://www.netopia.com/support/.

Appendix B

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia R910 and using some of its powerful features, such as static routes and packet filtering.

In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

This section covers the following topics:

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate.

Note: This guide uses the term "IP" in a very general and inclusive way to identify all of the following:

- Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP
- Packets that include an IP header within their structure
- Devices that send IP packets

About IP addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.168.1.1 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations that request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1–127	127	16,777,214	net.host.host.host	97.3.14.250
B	128–191	16,384	65,534	net.net.host.host	140.100.10.11
C	192–223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP routers, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits in order to leave room for the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP routers and gateways such as the Netopia R910.

Note: If you receive a routed account from an ISP, there must be a mask associated with your network IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

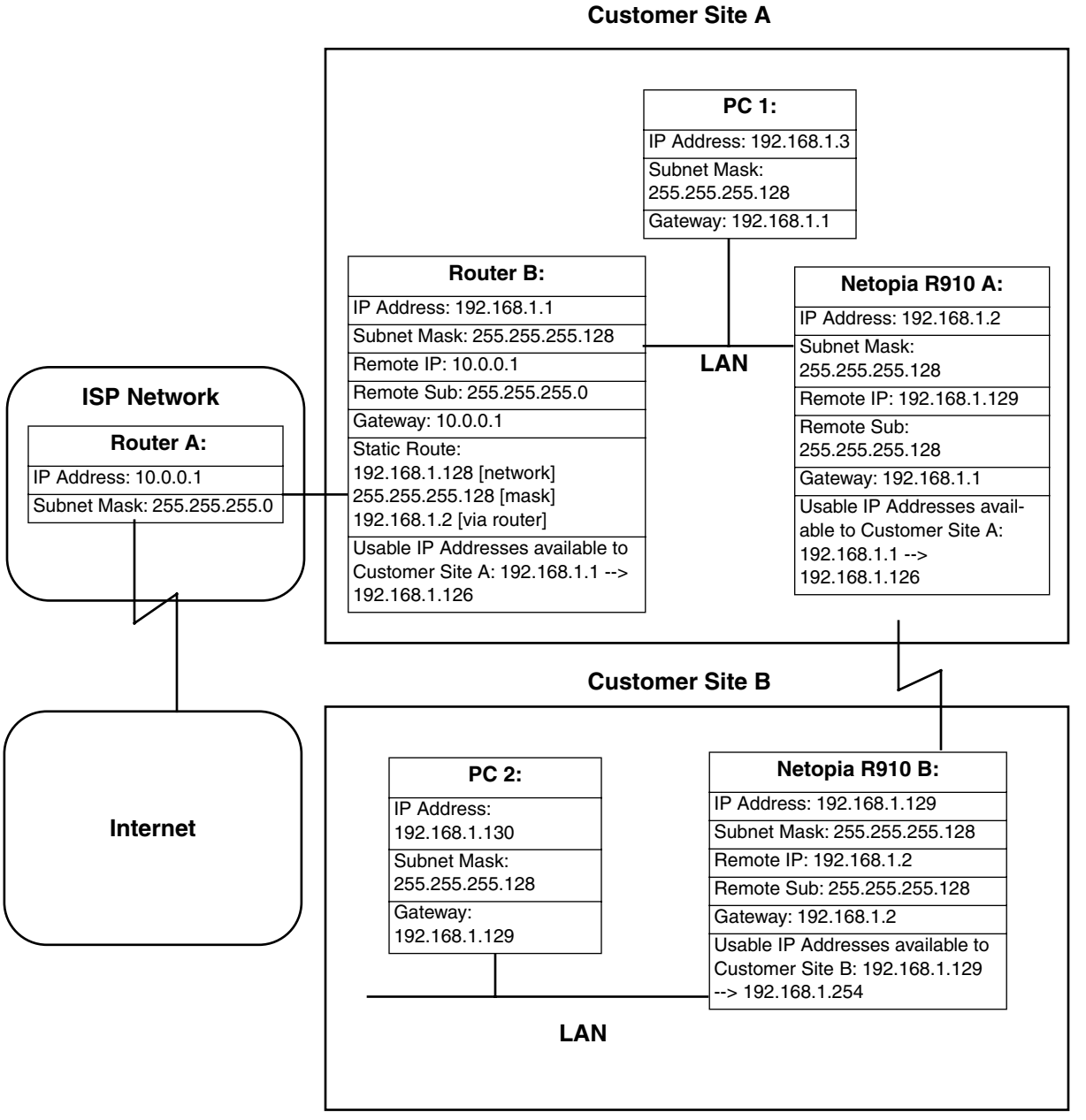
To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

When setting up IP routing with a Class A Address, or even with multiple Class C Addresses, subnetting is fairly straightforward. Subnetting a single Class C address between two networks, however, is more complex. This section describes the general procedures for subnetting a single Class C network between two Netopia routers so that each can have Internet access.

Network configuration

Below is a diagram of a simple network configuration. The ISP is providing a Class C address to the customer site, and both networks A and B want to gain Internet access through this address. Netopia R910 B connects to Netopia R910 A and is provided Internet access through Routers A and B.



Background

The IP addresses and routing configurations for the devices shown in the diagram are outlined below. In addition, each individual field and its meaning are described.

The IP Address and Subnet Mask fields define the IP address and subnet mask of the device's Ethernet connection to the network while the Remote IP and Remote Sub fields describe the IP address and subnet mask of the remote router. This information is entered in the connection profile of the Netopia R910.

The Gateway field describes the router or workstation's default gateway, or where they will send their packets if the appropriate route is not known. The Static Route field, which is only shown on Router B, tells Router B what path to take to get to the network defined by Netopia R910 B. Finally, the Usable IP Address field shows the range of IP addresses available to the hosts of that network.

Note that the IP addresses given in this section are for example purposes only. Do not use these addresses when configuring your network.

With this configuration, both Customer Site A and B can gain Internet access through Routers A and B, with no reconfiguration of the ISP's equipment. The most important item in this configuration is the static route defined on Router B. This tells Router B what path to take to get to the network defined by Netopia R910 B. Without this information, Customer Site B will be able to access Customer Site A, but not the Internet.

If it is not possible to define a static route on Router B, RIP could be enabled to serve the same purpose. To use RIP instead of a static route, enable Transmit RIP on Netopia R910 A and Transmit and Receive RIP on Router B. This will allow the route from Customer Site B to propagate on Router B and Customer Site A.

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts, and no plans to add any new hosts. You don’t need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you might obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP’s network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages of this situation are the greater ease and lower cost of obtaining a subnet rather than a full Class C address from an ISP.

Distributing IP addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an Internet service provider. When configuring the Netopia R910, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

There are two schemes for distributing the remaining IP addresses:

- Manually give each computer an address
- Let the Netopia R910 automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Netopia R910. Using the router in this way allows it to function as an address server.

One reason to use the Netopia R910 as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You need to enter information only once, rather than having to repeatedly enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Netopia R910 as an address server is that it will distribute addresses only to hosts that need to use them.

All Netopia R910s come with an integrated Dynamic Host Control Protocol (DHCP) server. Some routers also come with a Macintosh Internet Protocol (MacIP) server. These servers provide a means of distributing IP addresses to either a Mac or PC workstation as needed.

When setting up the DHCP or MacIP servers in the Netopia R910, it is necessary to understand how workstations lease, renew, and release their IP addresses. This information is helpful in determining dynamic address allocation for a network.

The term "lease" describes the action of a workstation requesting and using an IP address. The address is dynamic and can be returned to the address pool at a later time.

The term "renew" refers to what the workstations do to keep their leased IP address. At certain intervals, the workstation talks to the DHCP or MacIP server and renews the lease on that IP address. This renewal allows the workstation to keep and use the assigned IP address until the next renewal period.

The term "release" refers to a situation where the workstation is no longer using its assigned IP address or has been shut down. IP addresses can be manually released as well. The IP address goes back into the DHCP or MacIP address pool to be reassigned to another workstation as needed.

Technical note on subnet masking

Note: The IP address supplied by the Netopia R910 will be a unique number. You may want to replace this number with a number that your ISP supplies if you are configuring the router for a static IP address. The automatic IP mask supplied by SmartStart is a Class C address. However, the Netopia R910 and all devices on the same local network must have the same subnet mask. If you require a different class address, you can edit the IP Mask field to enter the correct address. Refer to the table below.

Number of Devices (other than Netopia R910) on Local Network	Largest Possible Ethernet Subnet Mask
1	255.255.255.252
2-5	255.255.255.248
6-13	255.255.255.240
14-29	255.255.255.224

Number of Devices (other than Netopia R910) on Local Network	Largest Possible Ethernet Subnet Mask
30-61	255.255.255.192
62-125	255.255.255.128
125-259	255.255.255.0

Configuration

This section describes the specific IP address lease, renew, and release mechanisms for both the Mac and PC, with either DHCP or MacIP address serving.

DHCP address serving

Windows 95 workstation:

- The Win95 workstation requests and renews its lease every half hour.
- The Win95 workstation does NOT relinquish its DHCP address lease when the machine is shut down.
- The lease can be manually expired using the WINIPCFG program from the Win95 machine, that is a command line program executable from the DOS prompt or from the START:RUN menu.

Windows 3.1 workstation (MSTCP Version 3.11a):

- The Win3.1 workstation requests and renews its lease every half hour.
- The Win3.1 workstation does NOT relinquish its DHCP address lease when the user exits Windows and goes to DOS.
- The lease can be manually expired by typing IPCONFIG/RELEASE from a DOS window within Windows or from the DOS prompt.

Macintosh workstation (Open Transport Version 1.1 or later):

- The Mac workstation requests and renews its lease every half hour.
- The Mac workstation relinquishes its address upon shutdown in all but one case. If the TCP/IP control panel is set to initialize at startup, and no IP services are used or the TCP/IP control panel is not opened, the DHCP address will NOT be relinquished upon shutdown. However, if the TCP/IP control panel is opened or if an IP application is used, the Mac WILL relinquish the lease upon shutdown.
- If the TCP/IP control panel is set to acquire an address only when needed (therefore a TCP/IP application must have been launched to obtain a lease) the Mac WILL relinquish its lease upon shutdown every time.

Netopia R910 DHCP server characteristics

- The Netopia R910 ignores any lease-time associated with a DHCP request and automatically issues the DHCP address lease for one hour.
- The number of devices a Netopia R910 can serve DHCP to is 512. This is imposed by global limits on the size of the address serving database, which is shared by all address serving functions active in the router.

- The Netopia R910 does release the DHCP address back to the available DHCP address pool precisely one hour after the last-heard lease request as some other DHCP implementations may hold on to the lease for an additional time after the lease expired, to act as a buffer for variances in clocks between the client and server.

MacIP serving

Macintosh workstation (MacTCP or Open Transport):

Once the Mac workstation requests and receives a valid address, the Netopia R910 actively checks for the workstation's existence once every minute.

- For a dynamic address, the Netopia R910 releases the address back to the address pool after it has lost contact with the Mac workstation for over 2 minutes.
- For a static address, the Netopia R910 releases the address back to the address pool after it has lost contact with the Mac workstation for over 20 minutes.

Netopia R910 MacIP server characteristics

The Mac workstation uses ATP to both request and receive an address from the Netopia R910's MacIP server. Once acquired, NBP confirm packets will be sent out every minute from the Netopia R910 to the Mac workstation.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer's address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That's why manually distributed addresses are sometimes called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. Appropriate candidates for a static address include: a network administrator's computer, a computer dedicated to communicating with the Internet, and routers.

Using address serving

The Netopia R910 provides two ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers. The third way, called Serve Dynamic WAN Clients (IPCP), is used to fulfill WAN client requirements

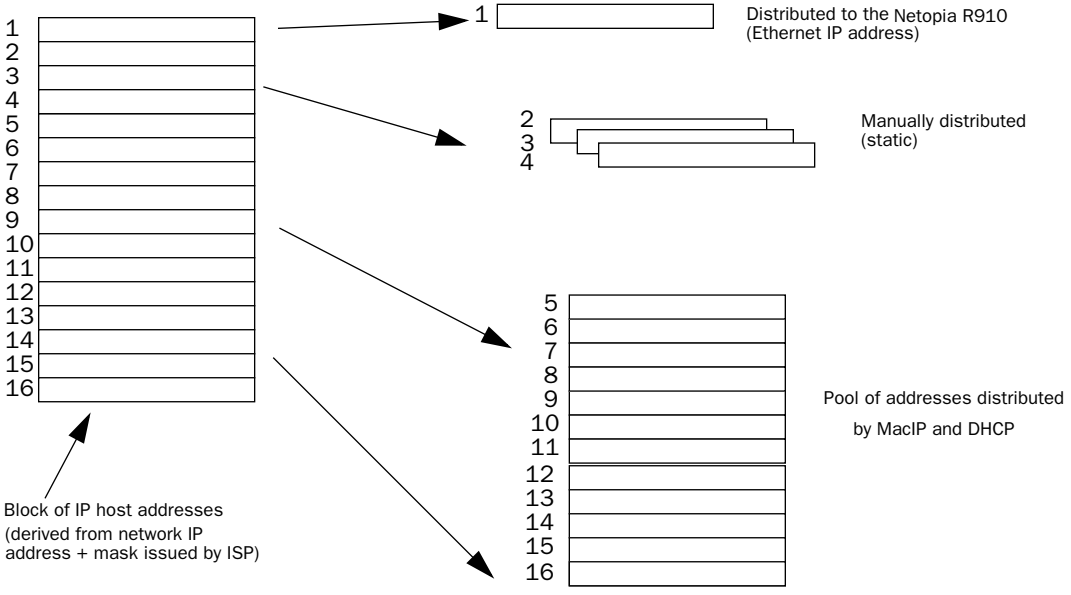
The Netopia R910 can use both DHCP and MacIP. Whether you use one or both depends on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Tips and rules for distributing IP addresses

- Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static

addresses.

- Note any planned and currently used static addresses before you use DHCP and MacIP.
- Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.



The figure above shows an example of a block of IP addresses being distributed correctly.

The example follows these rules:

- An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.
- A single IP address range is used by all the address-served clients. These include DHCP, BootP, MacIP, and WAN clients, even though BootP and static MacIP clients might not be considered served.
- The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.
- The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32 and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter "10" in the DHCP Setup screen's **Number of Addresses to Allocate** item. Then, in the same screen's **First Address** item, enter the first address in the sub-block to allocate so that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51).

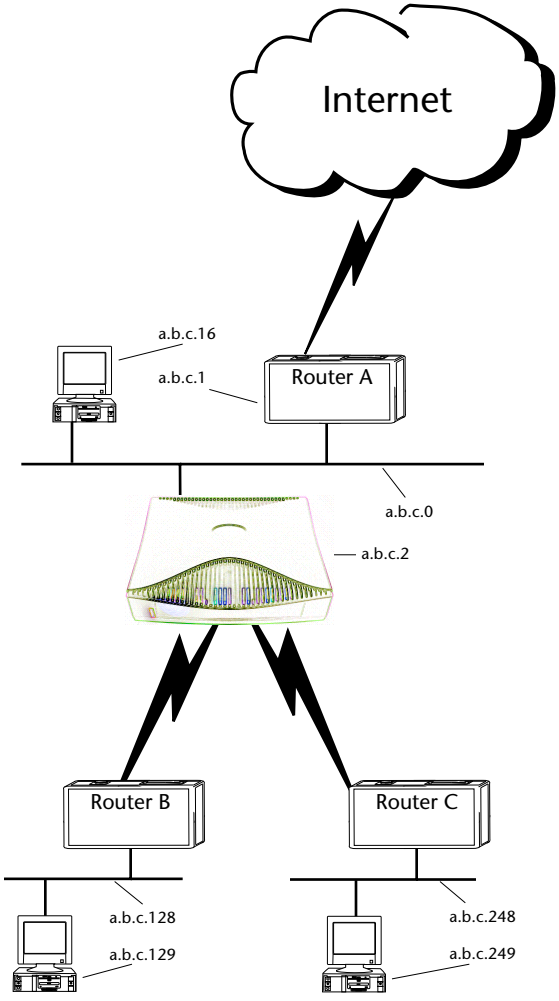
Nested IP subnets

Under certain circumstances, you may want to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses available to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network, while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

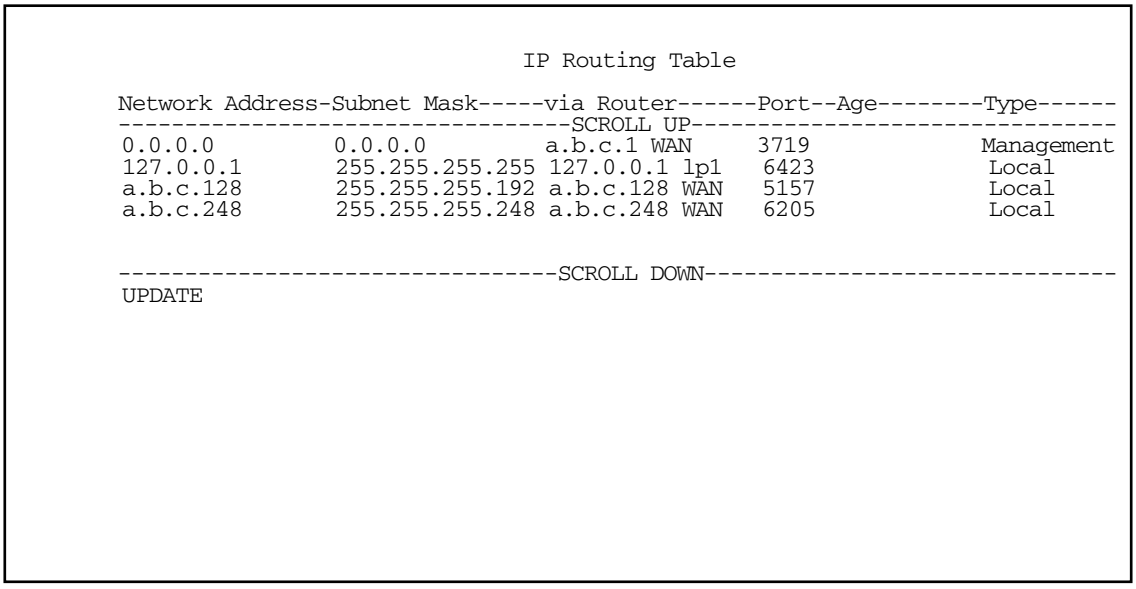
The figure at left shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Netopia R910), a Netopia R910, and a number of other hosts. Router A maintains a link to the Internet, and can be used as the default gateway.



Routers B and C (which could also be Netopia R910s) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Netopia R910 with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
For Router B	a.b.c.128	255.255.255.192	7
For Router C	a.b.c.248	255.255.255.248	3

The Netopia R910's connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:

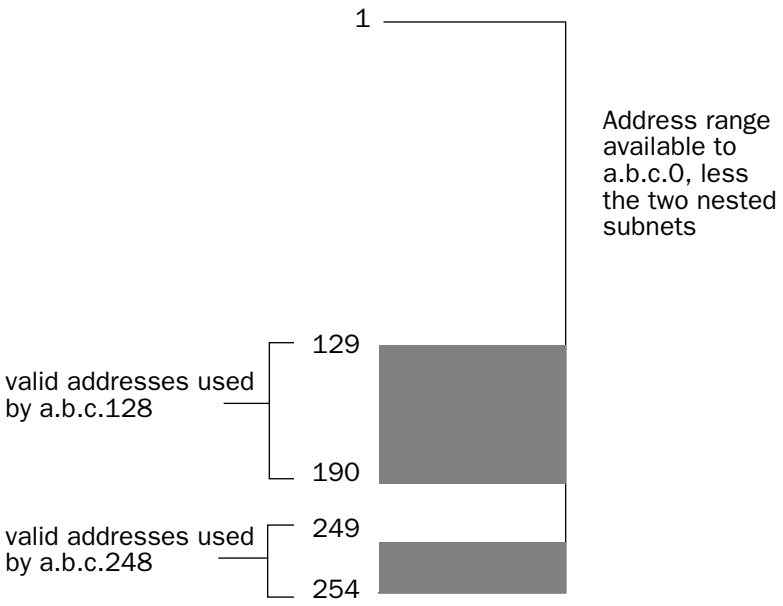


Let's see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Netopia R910, which examines its destination IP address.

The Netopia R910 compares the packet's destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there's a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route's subnet mask, it yields a.b.c.248, which matches the network address in the route. The Netopia R910 uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.



Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork if the host address is all ones or all zeros but the subnet address is a combination or zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. By default, the Netopia R910 uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

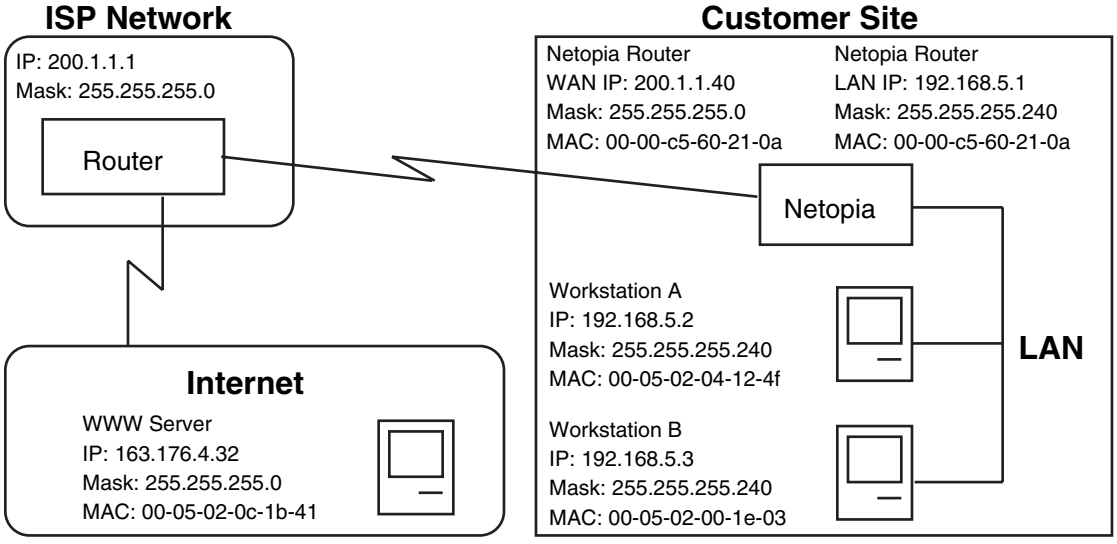
Appendix C

Understanding Netopia NAT Behavior

This appendix describes how Network Address Translation (NAT) works within the Netopia R910. The Netopia R910 implements a powerful feature called Network Address Translation as specified in RFC 1631. NAT is used for IP address conservation and for security purposes since there will only be a single IP "presence" on the WAN. This appendix describes the NAT functionality within the Netopia R910 and provides examples for setup and use.

Network configuration

Below is a diagram of the network referenced in this appendix.



Background

NAT is a mechanism employed within the Netopia R910 to acquire a statically or dynamically assigned IP address on its WAN interface and proxy against locally assigned IP addresses on its LAN interface. The Netopia R910 uses a one-to-many IP address mapping scheme; that is against a single IP address the Netopia R910 acquires on its WAN interface, the Netopia R910 can proxy 14, 30, or an unlimited number of IP hosts on the LAN interface.

In order to fully understand how NAT works, you must understand how a connection is established and IP addresses are negotiated.

When the Netopia R910 establishes a connection over its WAN interface with another router it uses the Point-to-Point Protocol (PPP). Within PPP there is a Network Control Protocol (NCP) called Internet Protocol Control Protocol (IPCP), which handles the negotiation of IP addresses between the two routers, in this case the Netopia R910 at the customer site above and the router at the Internet service provider (ISP).

If the Netopia R910 calls the router at the ISP with NAT disabled, the Netopia negotiates its LAN interface address (as specified in IP Setup within the Netopia R910's console) with the router at the ISP through IPCP and then sets up routing. From the diagram on the previous page you can see that the address for the Netopia R910 is 192.168.5.1 and the address of the router at the ISP is 200.1.1.1. Assuming that the addresses negotiated by the routers are valid and unique for the Internet, the Netopia R910 and the hosts on its LAN would be able to access the Internet.

If the Netopia R910 calls the router at the ISP with NAT enabled, instead of negotiating the LAN interface address, the Netopia R910 suggests the address 0.0.0.0 through IPCP. When the router at the ISP sees this all-zeros IPCP request, the router can either pull a free dynamic IP address from its pool and assign it to the Netopia R910's WAN interface or, if configured to do so, it can match the Netopia R910's incoming connection profile and assign a preconfigured static IP address to the Netopia R910's WAN interface.

From the diagram, you can see that the IP address assigned to the Netopia R910's WAN interface is 200.1.1.40, while the IP address assigned to the LAN interface remains the same. The LAN interface address 192.168.5.1 is thus hidden from the ISP and the Internet, and the Netopia R910 only has a single valid IP presence on the Internet. The LAN interface IP address for the Netopia R910 can be any IP address; however, it is recommended that you use the IANA-specified 192.168.X.X Class C address range, which is used for networks not attached to the Internet. This address range is described in RFC 1597.

The dynamic IP address acquisition on the WAN interface of the Netopia R910 is one of several features of NAT. Another is the mapping of locally assigned IP addresses to the single globally unique IP address acquired by the Netopia R910 on its WAN interface. NAT employs several things to accomplish this seamlessly. You must look at the formatting of an IP packet before IP address remapping can be explained.

Every IP packet that is transmitted across the Netopia R910's LAN interface or across the WAN interface to the Internet contains several bits of information that indicate to any device where the packet is going and where it came from. In particular, you have the source and destination port and source and destination IP addresses.

A port is used within IP to define a particular type of service and could be either a Transmission Control Protocol (TCP) port or User Datagram Protocol (UDP) port. Both TCP and UDP are protocols that use IP as the underlying transport mechanism. The major difference between TCP and UDP is that TCP is a reliable delivery service, whereas UDP is a "best-effort" delivery service. A list of well-known TCP or UDP ports and services can be found in RFC 1700.

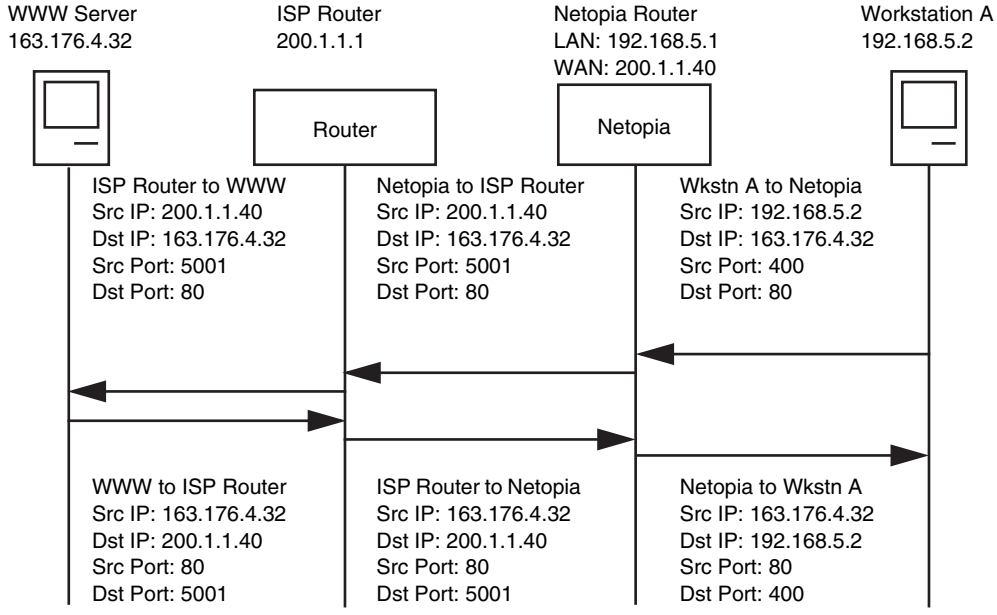
If Workstation A wants to communicate with a World Wide Web (WWW) server on the Internet and the Netopia R910 does not have NAT enabled, Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32. The source port could be 400 while the destination port would be 80 (WWW server). The Netopia R910 then looks at this IP packet, determines the best routing method and sends that packet on its way across the WAN interface to the WWW server on the Internet.

With NAT enabled, the Netopia R910 does something different. For example, suppose that Workstation A again wants to communicate with the WWW server on the Internet. Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32, and source port could be 400 while the destination port would be 80 (WWW server).

When the Netopia R910 receives this IP packet, it cannot simply forward it to the WAN interface and the Internet since the IP addresses on the LAN interface are not valid or globally unique for the Internet. Instead, the Netopia R910 has to change the IP packet to reflect the IP address that was acquired on the WAN interface from the ISP.

The Netopia R910 will first substitute the source IP address with the IP address that was acquired on the WAN interface, which in this case is 200.1.1.40. Next the Netopia R910 will substitute the source TCP or UDP port with a TCP or UDP port from within a specified range maintained within the Netopia R910. And finally the modified IP packet's checksum is recalculated (as specified in RFC 1631) and the packet is transmitted across the WAN interface to its destination, the WWW server on the Internet.

If the send and response IP packets were drawn out, this process would look like the following:

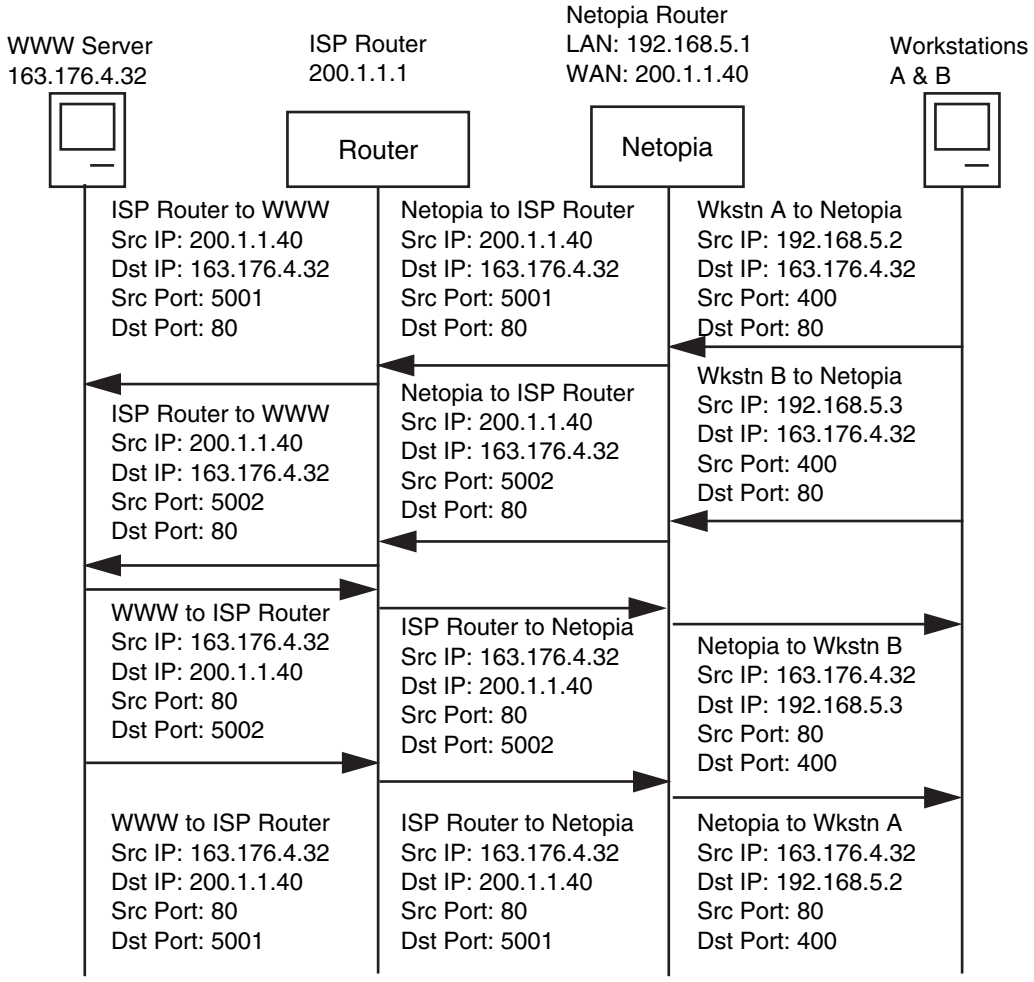


As you can see, the IP packet from Workstation A is sent to the Netopia R910 and the source IP address is substituted with 200.1.1.40 and the source port is substituted with 5001, then the IP packet checksum is recalculated. When this modified packet reaches the WWW server on the Internet, the WWW server responds and sends the IP packet back to destination IP address 200.1.1.40 and destination port 5001.

When the Netopia R910 receives this IP packet from the WWW server, the Netopia R910 replaces the destination IP address with 192.168.5.2, the address for Workstation A. The port is changed back to 400, the IP packet checksum is recalculated, and the IP packet is sent to Workstation A on the Netopia R910s LAN interface.

The reasons for the IP address changes are obvious from the preceding diagram, but what is not so obvious is why the TCP or UDP source ports need to be changed as well. These are changed and maintained in an internal table so the Netopia R910 can determine which host on the local LAN interface sent the IP packet and what host the response from the WAN interface is going to go to on the LAN interface. This becomes especially important when two or more hosts on the LAN interface are accessing the same type of service on the Internet, like a WWW server (port 80), for example.

Now look at how two hosts on the LAN interface accessing the same WWW server on the Internet will work:



As you can see, when Workstation A and Workstation B transmit an IP packet to the WWW server on the Internet, they have unique source IP addresses on the LAN interface but potentially the same source ports, which in this case is 400. When the Netopia R910 receives these packets, the source IP addresses are substituted with the single globally unique IP address that was acquired on the WAN interface, which is 200.1.1.40.

Now both IP packets have the exact same source IP address (200.1.1.40) and source ports (400). The Netopia R910 is then able to distinguish between the two IP packets by changing the source TCP or UDP ports and keeping this information in an internal table. As seen above, the source port for Workstation A has been changed to 5001 and the source port for Workstation B has been changed to 5002.

If you were to look at the internal port mapping table that is maintained by the Netopia R910, it would look similar to the following:

Source LAN IP	Source LAN Port	Remapped LAN Port
192.168.5.2	TCP 400	TCP 5001
192.168.5.3	TCP 400	TCP 5002

With this information the Netopia R910 can determine the appropriate routing for an IP response from the Internet. In this case, when the WWW server responds with a destination port of 5001, the Netopia R910 can see that this packet's destination on the local LAN interface is actually Workstation A at IP address 192.168.5.2. Likewise, with the response for port 5002, the Netopia R910 can see that this packet's destination on the local LAN interface is actually Workstation B at IP address 192.168.5.3.

Exported services

Note that this “automatic” port remapping and IP address substitution only works in one direction – for IP packets that originated on the LAN interface destined to the WAN interface and the Internet. In order for port remapping and IP address substitution to work in the other direction – that is, hosts on the Internet that want to originate an IP packet destined to a host on the Netopia R910s LAN interface – a manual redirection of TCP or UDP ports as well as destination IP addresses within the Netopia R910 is required. This manual port remapping and IP address substitution is accomplished by setting up exported services.

Exported services are essentially user-defined pointers for a particular type of incoming TCP or UDP service from the WAN interface to a host on the local LAN interface. This is necessary since the Netopia R910 and thus the attached local LAN has only one IP presence on the WAN interface and Internet. Exported services allows the user to redirect one type of service – for example Port 21 (FTP) – to a single host on the local LAN interface. This will then allow the Netopia R910 to redirect any packets coming in from the Internet with the defined destination TCP or UDP port of port 21 (FTP) to be redirected to a host on the local LAN interface.

For example, suppose the WWW server on the Internet with the IP address of 163.176.4.32 wants to access Workstation B on the Netopia R910s local LAN interface which is operating as an FTP server. The IP address for Workstation B is 192.168.5.3, which is not a valid IP address, and thus the WWW server on the Internet cannot use this IP address to access Workstation B.

The WWW server on the Internet would then have to use the single valid IP address that was acquired on the Netopia R910's WAN interface to access any host on the Netopia R910's local LAN interface, since this is the only valid address for the Internet. But if the WWW server on the Internet opens a connection to 200.1.1.40 via port 21 (FTP) and no exported services are defined on the Netopia R910, the Netopia R910 will discard the incoming packet since the Netopia R910 itself does not perform the requested service.

You can see why exported services are necessary. In the example above, an Exported Service needs to be defined within the Netopia R910 redirecting any incoming IP traffic with a destination port of 21 to the host on the local LAN interface with the IP address of 192.168.5.3.

If the WWW server on the Internet then tries to open a connection to the IP address of 200.1.1.40 with the appropriate Exported Service defined, the Netopia R910 will look at the destination port and will find that it is destined for port 21 (FTP). The Netopia R910 then looks at the internal user-defined exported services table and finds that any incoming IP traffic from the WAN port with a destination of port 21 (FTP) should be redirected to the IP address of 192.168.5.3 on the local LAN interface, which in this case is Workstation B.

Once the appropriate exported services are defined, there can be seamless communication between a host on the Internet and a host on the Netopia R910's local LAN interface.

Important notes

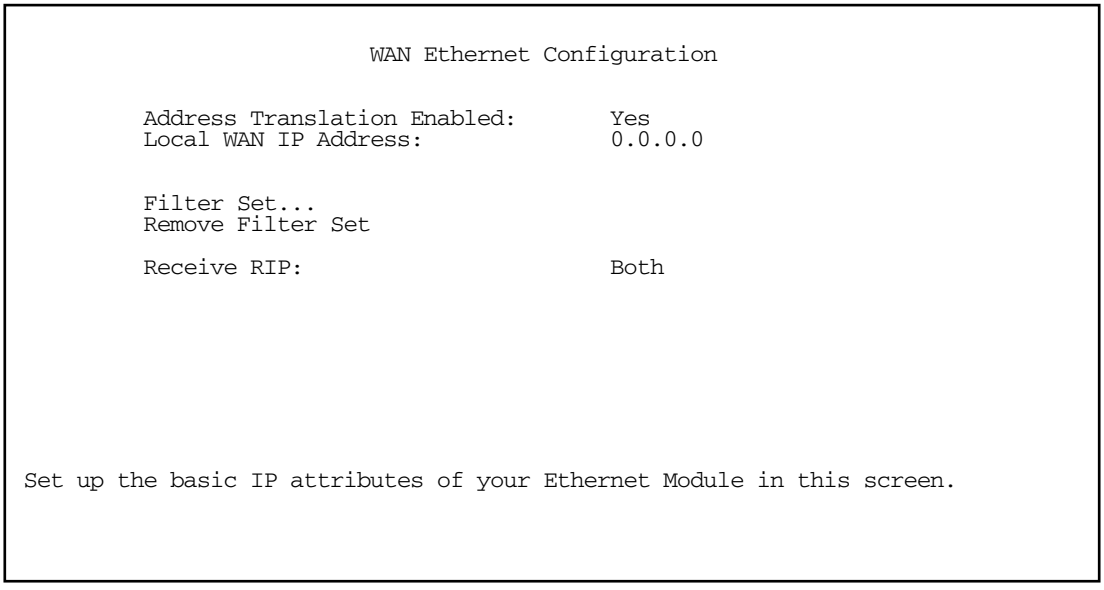
Even with the advantages of NAT, there are several things you should note carefully:

- There is no formally agreed-upon method among router vendors for handling an all-zeros IPCP request. The majority of router vendors use the all-zeros IPCP request to determine when a dial-in host wants to be assigned an IP address. Some vendors however attempt to negotiate and establish routing with an all-zeros IP address. The Netopia R910 will not allow routing to be established with an all-zeros IP address and the call will be dropped with an error logged in the Device Event History.
- When using NAT it is most likely that the Netopia R910 will be receiving an IP address from a "pool" of dynamic IP addresses at the ISP. This means that the Netopia R910's IP presence on the Internet will change with each connection. This can potentially cause problems with devices on the Internet attempting to access services like WWW and FTP servers or AURP partners on the Netopia R910's local LAN interface. In this case, if a dynamic IP address is assigned to the WAN interface of the Netopia R910 each time, the administrator of the Netopia R910 will have to notify clients who want to access services on the Netopia R910's LAN interface of the new IP address after each connection.
- With NAT enabled, there cannot be two or more of the same types of service accessible from the Internet on the LAN interface of the Netopia R910. For example, there cannot be multiple FTP servers (Port 23) on the Netopia R910's LAN interface that can be accessible by workstations on the Internet. This is because there is no way within the Netopia R910 and IP to distinguish between multiple servers using the same port, in this case port 23.
- Fictional IP addresses may be assigned on the Netopia R910's LAN interface. It is strongly recommended that for the Netopia R910's LAN interface, an IP address from the Class C address range of 192.168.X.X be used. This is because this range is defined by the IANA as an address space that will never be routed through the Internet and is to be used by private Intranets not attached to the Internet.

  If the address range of 192.168.X.X is not used and another range of addresses such as 100.1.1.X is used instead, this address space can potentially overlap an address space that is owned by a user attached to the Internet. Thus if a user on the Netopia R910's LAN interface has an IP address of 100.1.1.2 while the Netopia R910's LAN interface is 100.1.1.2 and the local host wants to access a host on the Internet with the address of 100.1.1.8, the Netopia R910 has no way of knowing that the 200.1.1.8 address is actually on the Internet and not on its local LAN interface, since the local LAN interface is assigned the IP address range of 200.1.1.1 to 200.1.1.14.

Configuration

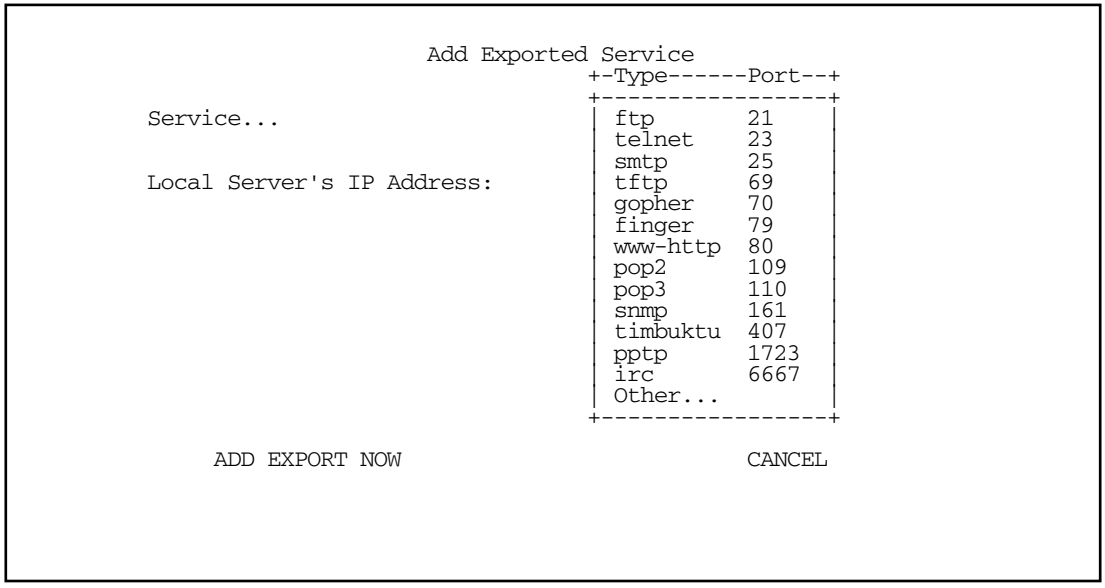
You can toggle **Address Translation Enabled** to No or Yes in the WAN Ethernet Configuration screen in WAN Configuration under the Main Menu. An example of enabling NAT is as follows:



Toggling Address Translation Enabled to Yes enables the Netopia R910 to send out an all-zeros IPCP address that requests an IP to be assigned to the Netopia R910's WAN interface. Note that the remote IP address is 127.0.0.2, which should also be the default gateway under IP Setup in System Configuration. This is done for profile matching purposes and because the IP address of the router the Netopia R910 is dialing is not always known.

As mentioned earlier in this appendix, NAT works well for IP sessions originated on the Netopia R910's LAN interface destined for the Internet without any additional configuration. For incoming IP connections from the Internet to a host on the Netopia R910's LAN interface, exported services need to be used.

Exported services are configured under IP Setup in System Configuration. This is where a particular type of TCP or UDP service originating from the Internet is redirected to a host on the Netopia R910's LAN interface. An example of this screen follows:



Within exported services is a pop-up list of well-known TCP and UDP services that can be redirected to a single host on the Netopia R910's LAN interface. There is also an "Other..." option that allows for manual configuration of additional TCP or UDP ports. There can be a total of 32 exported services that can be defined.

When a particular type of service is redirected to an IP address, that service is removed from the pop-up list, since only one type of service can be redirected to a single host. However several different types of services can be redirected to a single or multiple hosts. For example, port 80 (WWW server) could be redirected to 192.168.5.3 on the Netopia R910's LAN interface, and port 23 (Telnet) can be redirected to that same host.

Summary

NAT is a powerful feature of the Netopia R910 and when used and set up properly can yield a secure network while only using one IP address on the WAN interface. Note that the addresses listed in this appendix are for demonstration purposes only. Do not use these addresses when configuring your local network.

Appendix D

Binary Conversion Table

This table is provided to help you choose subnet numbers and host numbers for IP and MacIP networks that use subnetting for IP addresses.

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
0	0	32	100000	64	1000000	96	1100000
1	1	33	1000001	65	1000001	97	1100001
2	10	34	100010	66	1000010	98	1100010
3	11	35	100011	67	1000011	99	1100011
4	100	36	100100	68	1000100	100	1100100
5	101	37	100101	69	1000101	101	1100101
6	110	38	100110	70	1000110	102	1100110
7	111	39	100111	71	1000111	103	1100111
8	1000	40	101000	72	1001000	104	1101000
9	1001	41	101001	73	1001001	105	1101001
10	1010	42	101010	74	1001010	106	1101010
11	1011	43	101011	75	1001011	107	1101011
12	1100	44	101100	76	1001100	108	1101100
13	1101	45	101101	77	1001101	109	1101101
14	1110	46	101110	78	1001110	110	1101110
15	1111	47	101111	79	1001111	111	1101111
16	10000	48	110000	80	1010000	112	1110000
17	10001	49	110001	81	1010001	113	1110001
18	10010	50	110010	82	1010010	114	1110010
19	10011	51	110011	83	1010011	115	1110011
20	10100	52	110100	84	1010100	116	1110100
21	10101	53	110101	85	1010101	117	1110101
22	10110	54	110110	86	1010110	118	1110110
23	10111	55	110111	87	1010111	119	1110111
24	11000	56	111000	88	1011000	120	1111000
25	11001	57	111001	89	1011001	121	1111001
26	11010	58	111010	90	1011010	122	1111010
27	11011	59	111011	91	1011011	123	1111011
28	11100	60	111100	92	1011100	124	1111100
29	11101	61	111101	93	1011101	125	1111101
30	11110	62	111110	94	1011110	126	1111110
31	11111	63	111111	95	1011111	127	1111111

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

Appendix E

Further Reading

Alexander, S. & R. Droms, *DHCP Options and BOOTP Vendor Extensions*, RFC 2131, Silicon Graphics, Inc., Bucknell University, March 1997.

Angell, David. *ISDN for Dummies* Foster City, CA: IDG Books Worldwide, 1995. Thorough introduction to ISDN for beginners.

Apple Computer, Inc. *AppleTalk Network System Overview*. Reading, MA: Addison-Wesley Publishing Company, Inc., 1989.

Apple Computer, Inc. *Planning and Managing AppleTalk Networks*. Reading, MA: Addison-Wesley Publishing Company, Inc., 1991.

Asymmetric Digital Subscriber Line (ADSL) Forum, *Framing and Encapsulation Standards for ADSL: Packet Mode*, TR-003, June 1997.

Black, U. *Data Networks: Concepts, Theory and Practice*. Englewood Cliffs, NJ: Prentice Hall, 1989.

Black, U. *Physical Level Interfaces and Protocols*. Los Alamitos, CA: IEEE Computer Society Press, 1988.

Black, Uyless. *Emerging Communications Technologies* Englewood Cliffs, NJ: PTR Prentice Hall, 1994. Describes how emerging communications technologies, including ISDN and Frame Relay, operate and where they fit in a computer/communications network.

Bradley, T., C. Brown & A. Malis, *Multiprotocol Interconnect over Frame Relay*, Network Working Group, Internet Engineering Task Force, RFC 1490, July 1993.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Introduction to the Simple Gateway Monitoring Protocol." *IEEE Network*: March 1988.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Network Management and the Design of SNMP." *ConneXions: The Interoperability Report*, Vol. 3: March 1989.

Chapman, D. Brent. “Network (In)Security Through IP Packet Filtering” Paper available from Great Circle Associates, 1057 West Dana Street, Mountain View, CA 94041.

Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls* Sebastopol, CA: O’Reilly & Associates, 1995. Dense and technical, but Chapter 6 provides a basic introduction to packet filtering.

Chappell, L. *Novell's Guide to NetWare LAN Analysis*. San Jose, CA: Novell Press, 1993.

Clark, W. "SNA Internetworking." *ConneXions: The Interoperability Report*, Vol. 6, No. 3: March 1992.

Comer, D.E. *Internetworking with TCP/IP: Principles, Protocols, and Architecture* Vol. I, 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1991.

Copper Mountain Networks, Internal Control Protocol (ICP) Interface Control Document (ICD), January 5, 1998.

Davidson, J. *An Introduction to TCP/IP*. New York, NY: Springer-Verlag, 1992.

Droms, R., *Dynamic Host Configuration Protocol*, RFC 2131, Bucknell University, March 1997.

Ferrari, D. *Computer Systems Performance Evaluation*. Englewood Cliffs, NJ: Prentice Hall, 1978.

Garcia-Luna-Aceves, J.J. "Loop-Free Routing Using Diffusing Computations." Publication pending in IEEE/ACM Transactions on Networking, Vol. 1, No. 1, 1993.

Garfinkel, Simson. *PGP: Pretty Good Privacy* Sebastopol, CA: O'Reilly & Associates, 1991. A guide to the free data encryption program PGP and the issues surrounding encryption.

Green, J.K. *Telecommunications*, 2nd ed. Homewood, IL: Business One Irwin, 1992.

Heinanen, J., *Multiprotocol Encpasulation over ATM Adaptation Layer 5*, RFC 1483, July 1993.

Jones, N.E.H., and D. Kosiur. *MacWorld Networking Handbook*. San Mateo, CA: IDG Books Worldwide, Inc., 1992.

Kousky, K. "Bridging the Network Gap." *LAN Technology*, Vol. 6, No. 1: January 1990.

LaQuey, Tracy. *The Internet Companion: A Beginner's Guide to Global Networking* Reading, MA: Addison-Wesley Publishing Company, 1994.

Leinwand, A., and K. Fang. *Network Management: A Practical Perspective*. Reading, MA: Addison-Wesley Publishing Company, 1993.

Levine, John R., and Carol Baroudi. *The Internet for Dummies* Foster City, CA: IDG Books Worldwide, 1993. Covers all of the most popular Internet services, including e-mail, newsgroups, and the World Wide Web. Also has information on setting up individual workstations with TCP/IP stacks.

Lippis, N. "The Internetwork Decade." *Data Communications*, Vol. 20, No. 14: October 1991.

McNamara, J.E. *Local Area Networks*. Digital Press, Educational Services, Digital Equipment Corporation, 12 Crosby Drive, Bedford, MA 01730.

Malamud, C. *Analyzing Novell Networks*. New York, NY: Van Nostrand Reinhold, 1991.

Malamud, C. *Analyzing Sun Networks*. New York, NY: Van Nostrand Reinhold, 1991.

Martin, J. *SNA: IBM's Networking Solution*. Englewood Cliffs, NJ: Prentice Hall, 1987.

Martin, J., with K.K. Chapman and the ARBEN Group, Inc. *Local Area Networks: Architectures and Implementations*. Englewood Cliffs, NJ: Prentice Hall, 1989.

Miller, A. Mark. *Analyzing Broadband Networks (Frame Relay, SMDS, & ATM)* M&T Books, San Mateo, CA, 1994. An intermediate/advanced reference on Frame Relay technologies.

Miller, M.A. *Internetworking: A Guide to Network Communications LAN to LAN; LAN to WAN*, 2nd. ed. San Mateo, CA: M&T Books, 1992.

Miller, M.A. *LAN Protocol Handbook*. San Mateo, CA: M&T Books, 1990.

Miller, M.A. *LAN Troubleshooting Handbook*. San Mateo, CA: M&T Books, 1989.

Perlman, R. *Interconnections: Bridges and Routers*. Reading, MA: Addison-Wesley Publishing Company, 1992.

Rose, M.T. *The Open Book: A Practical Perspective on OSI*. Englewood Cliffs, NJ: Prentice Hall, 1990.

Rose, M.T. *The Simple Book: An Introduction to Management of TCP/IP-based Internets*. Englewood Cliffs, NJ: Prentice Hall, 1991.

Schwartz, M. *Telecommunications Networks: Protocols, Modeling, and Analysis*. Reading, MA: Addison-Wesley Publishing Company, 1987.

Sherman, K. *Data Communications: A User's Guide*. Englewood Cliffs, NJ: Prentice Hall, 1990.

Sidhu, G.S., R.F. Andrews, and A.B. Oppenheimer. *Inside AppleTalk,* 2nd ed. Reading, MA: Addison-Wesley Publishing Company, 1990.

Siyan, Karanjit. *Internet Firewall and Network Security* Indianapolis, IN: New Riders Publishing, 1995. Similar to the Chapman and Zwicky book.

Smith, Philip. *Frame Relay Principles and Applications* Reading, MA: Addison-Wesley Publishing Company, 1996. Covers information on Frame Relay, including the pros and cons of the technology, description of the theory and application, and an explanation of the standardization process.

Spragins, J.D., et al. *Telecommunications Protocols and Design*. Reading, MA: Addison-Wesley Publishing Company, 1991.

Stallings, W. *Data and Computer Communications*. New York, NY: Macmillan Publishing Company, 1991.

Stallings, W. *Handbook of Computer-Communications Standards,* Vols. 1–3. Carmel, IN: Howard W. Sams, 1990.

Stallings, W. *Local Networks*, 3rd ed. New York, NY: Macmillan Publishing Company, 1990.

Stevens, W.R. *TCP/IP Illustrated*, Vol 1. Reading, MA: Addison-Wesley Publishing Company, 1994.

Sunshine, C.A. (ed.). *Computer Network Architectures and Protocols*, 2nd ed. New York, NY: Plenum Press, 1989.

Tannenbaum, A.S. *Computer Networks*, 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1988.

Terplan, K. *Communication Networks Management*. Englewood Cliffs, NJ: Prentice Hall, 1992.

Tsuchiya, P. "Components of OSI: IS-IS Intra-Domain Routing." *ConneXions: The Interoperability Report*, Vol. 3, No. 8: August 1989.

Tsuchiya, P. "Components of OSI: Routing (An Overview)." *ConneXions: The Interoperability Report*, Vol. 3, No. 8: August 1989.

Zimmerman, H. "OSI Reference Model–The ISO Model of Architecture for Open Systems Interconnection." *IEEE Transactions on Communications COM-28*, No. 4: April 1980.

Appendix F

Technical Specifications and Safety Information

Description

Dimensions: 124.0 cm (w) x 20.0 cm (d) x 5.3 cm (h)
9.4” (w) x 7.9” (d) x 2.1” (h)

Communications interfaces: The Netopia R910 Ethernet Router has an RJ-45 jack for Ethernet line connections; a 4–port 10Base-T Ethernet hub for your LAN connection; and a DB-9 Console port.

Power requirements

- 12 VDC input
- 1.5 amps

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% noncondensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via XMODEM or TFTP

Routing: TCP/IP Internet Protocol Suite, RIP

WAN support: Ethernet

Security: IP firewall, UI password security

SNMP network management: SNMPv1, MIB-II (RFC 1213), Interface MIB (RFC 1229), Ethernet MIB (RFC 1643), Netopia R910 MIB

Management/configuration methods: serial console, Telnet, SNMP

Diagnostics: Ping, event logging, routing table displays, traceroute, statistics counters, Web-based management

Agency approvals

The Netopia R910 Ethernet Router has met the safety standards (per CSA-950) of the Canadian Standards Association for Canada.

The Netopia R910 Ethernet Router has met the safety standards (per UL-1950) of the Underwriters Laboratories for the United States.

Regulatory notices

Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

United States. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Service requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or our of warranty. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 2470 Mariner Square Loop, Alameda, California, 94501.

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Declaration for Canadian users

The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The load number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop that is used by the device to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the load numbers of all the devices does not exceed 100.

Important safety instructions

Caution

- The direct plug-in power supply serves as the main power disconnect; locate the direct plug-in power supply near the product for easy access.
- For use only with CSA Certified Class 2 power supply, rated 12VDC, 1.5A.

Telecommunication installation cautions

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

Battery

The Netopia R910's lithium battery is designed to last for the life of the product. The battery is not user-serviceable.

Caution!

Danger of explosion if battery is incorrectly replaced.

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Index

V

W

X